Courts Ill-Equipped To Police Cyber Threats And Cyberbullying In The Anonymous Age

by: **Kenneth Linzer**

Comment

Image Credits: blvdone / Shutterstock

Kenneth A. Linzer
Contributor

Editor's note: *Kenneth A. Linzer is a partner at Linzer Law Group, PC who counsels executives, business owners, and boards of directors in matters including strategic planning and corporate governance.*

Anonymous messaging apps, including Yik Yak, Whisper and Secret, have become a disturbing element of the cyber landscape. These anonymizing apps are quickly becoming a fact of life for schools, parents, children and many other groups in our present day social media scene.

Yik Yak, which received $62 million from Sequoia last month, and similar anonymizing apps have been blamed for school closures, threats to otherwise peaceful neighborhoods, and yet unidentified risks to our society. Yik Yak has a limited geographic perimeter of 1.5 miles and was designed for college-age users on college campuses as a virtual bulletin board. However, it's been used by those much younger and less mature.

Hardly a week goes by without another story of cyber threats against our public institutions or cyberbullying against our youth, often with significant costs to businesses, public service providers or innocent young victims.

The surprising fact is that the majority of cyber threats are perpetrated by adolescent boys, while cyberbullying is perpetrated by groups of two or more adolescent or pre-adolescent girls. While the more extreme cyber threats and cyberbully stories make the headlines, the costs to businesses, public facilities and youth often go unaccounted for.

These stories demonstrate the need for more informed and remedial measures by our legislatures and judicial system. Public facilities and institutions must be able to identify, respond to, and stop these cyber threats and cyberbullying before further damage occurs. Courts must become more knowledgeable about, and better equipped to address, this growing problem. Authorizing courts to address cyber threats and cyberbullying should not be a difficult challenge, but it is made more difficult due to these anonymity apps.

Commentators frequently provide tips to victims with the simple advice to block the cyber attacker's messages, emails or texts. Easy to do when you have an email address or phone number; not so easy when the cyberattack is transmitted anonymously. A victim could change their phone number or social media account (as

one unsympathetic judge recently advised); but, how long will this fix last in a junior high or high school environment, where social connections are not only a primary focus, but the focus for these adolescents and pre-adolescents? Any permanent solution requires the ability to easily identify the source of the cyberthreat or cyberbullying.

Recently, my firm discovered how ill-equipped our court system is to deal with such threats when we needed to respond immediately to a cyberbullying situation. Although the context was individual, it clearly exposed the problem that any business, government agency or public institution faces when having to seek assistance from the courts to combat a cyber threat or cyberbullying.

We were asked to discover the identity of the person who had sent a prominent client's pre-teen daughter, "Alice," an anonymous text threatening to falsely accuse her of being a member of the LGBT community, which she wasn't, using one of these apps. Suspecting who had sent the text, Alice showed it to her parents. Alice's school had a no-tolerance policy for cyber threats or cyberbullying; but before the school or police could act, Alice needed to identify the suspected cyberbully. This is not an easy task when senders mask their identities using an anonymizing app or text service.

Many of these anonymizing apps prohibit the posting or sending of harassing or abusive messages or texts from their sites or using their apps, cautioning users that they will assist victims of such practices by providing the IP address and time stamp associated with the abusive text. An IP address alone, however, is not enough.

The Internet is full of IP geolocation sites, merely providing a general location of an IP address and the name of the ISP for that address. Through the use of this type of geolocating website, we narrowed our

search to one Los Angeles area served by a large cable ISP. Then our adventures down this rabbit hole began.

The case of Alice

In initially dealing with the cable ISP, we encountered the first major roadblock – the Cable Privacy Act, which prohibits the disclosure of "personally identifiable information" of cable subscribers to the average person without a court order and notice to the subscriber.

Next, Alice enters the world of the unknown. The most efficient method for obtaining a court order to identify and restrain the perpetrator was to apply to the Los Angeles Superior Court Civil Harassment Department — or so we thought. We were informed, however, that a court order or restraining order could only be issued against known persons. Alice was free to file a Los Angeles Superior Court complaint, thereby initiating the process of obtaining discovery of her cyberbullies, or go to the police, which the family chose not to do, thus shielding their daughter from the criminal justice system.

Alice then falls down the rabbit hole of litigation. We sought a court order to require the cable ISP to provide the identity associated with the IP address from which the anonymous text originated. The first judge was unsympathetic to our pre-teen's ordeal, advising us to "have the girl get a new phone number and don't give it to anyone." Not the most practical advice for this mobile era.

Cyberthreat perpetrators and cyberbullies have all the tools they need to launch their attacks; victims should have the tools

they need to defend themselves.

But Alice discovers another path. A subpoena was served on the cable ISP, which ordinarily would have the same effect of a court order; but not according to this cable ISP. They'd have no problem responding to a court order, but would not respond to a mere subpoena.

Alice then returns to court. We next appeared ex parte for a court order compelling the cable ISP to respond to the subpoena (a step that the ISP did not oppose). The court issued the order, requiring the ISP to identify the subscriber of that IP address after notifying their subscriber under 47 U.S.C. § 551(c)(2)(B) that their identity was being sought, and advising them of a 10-day period to object to their identify being provided to the requesting party.

We waited. Finally, several months and tens of thousands of dollars later, we obtained the identity of the subscriber associated with the IP address.

With that information in hand, Alice's parents approached the school administrators. Not surprisingly, the identified classmates first denied having sent the offensive text and then, pointed the finger at one another, without ever admitting their bad acts. However the evidence was undeniable. Alice was fortunate that her family was able to afford the lengthy and expensive process. Not all victims have the resources available.

Quicker to identify

Our courts must have a quicker, more efficient means of obtaining identifying information in cases of cyberthreats or cyberbullying. One solution is to allow the Civil Harassment Department to issue the needed order to ISPs where victims demonstrate good cause without requiring the full process of filing a lawsuit and

issuing a subpoena. This reduces both costs and time by not requiring the filing of a complaint, the servicing of a subpoena, having that subpoena ignored and having to seek a court order to fulfill what should be a simple request.

Cyberthreat perpetrators and cyberbullies have all the tools they need to launch their attacks; victims should have the tools they need to defend themselves. A streamlined method for obtaining identifying information from ISPs would remove the current barriers, bring cyberthreat perpetrators and cyberbullies into the light, and avoid others having to follow in Alice's footsteps in their own adventures in Wonderwholand.