EDUCATION WEEK

COMMENTARY

Cyberbullies Can Easily Outwit Our Legal System

By Kenneth A. Linzer

Hardly a week goes by without another story of cyberbullying and the devastating emotional damage inflicted on its innocent young victims, a majority of whom are adolescent and pre-adolescent girls. While the tragic consequences of some of these attacks make headlines, the psychic trauma experienced by many victims is suffered silently, and may last for years.

These stories demonstrate the need for engaged, supportive parents (both of the cyberbully and the cyberbullied); schools able to identify, respond to, and stop cyberbullying before further damage occurs; and knowledgeable courts equipped to address a pernicious and growing social problem.

Our judicial system, however, has been slow to find its footing in this arena. And the task becomes more difficult as technology offers up a wider array of tools for anonymity in the cyber forum.

—Cari Vander Yacht for Education Week

All of us have received spam or phishing emails from fake or rerouted email accounts. But some may not realize that anyone can send a text from an email account masking his or her true identity. There's even a wikiHow page with **step-by-step instructions** on how to do it. For those who don't want to go through the effort of setting up a fake email account, websites such as textem.net and sendanonymoustext.com will allow them to send an anonymous text from a simple online interface. And there are a number of apps that allow anonymous texting right from the cyberbully's smartphone.

Of course, there are also websites and commentators that provide tips and counseling to cyber victims. But much of their advice boils down to this: Block the cyberbully's emails or texts. Easy to do when the attacker has a known email address or phone number. Not so easy when the cyberattack is transmitted anonymously. A victim could change her own phone number or social-media account—advice given by one unsympathetic judge recently. But how long would this fix last in a junior high or high school environment, where social connections are a primary focus? Any lasting solution has to involve an open dialogue with parents and school administrators. The first step in that dialogue, however, is often the most difficult—identifying the cyberattacker.

Our law firm learned this firsthand recently, when we responded to a client's plea for help in confronting a cyberbully. Her young daughter, a gifted student at one of the country's best private schools, had been the victim of a traumatic series of offensive online posts. Our client sought our help in finding the identity of the person or persons who had sent these lurid anonymous texts to the 11-year-old, through the anonymizing website textem.net. The girl (we'll call her Alice) was devastated after receiving the most defamatory text. Suspecting who had sent it, she wisely showed it to her parents.

Alice is more fortunate than many cyberbullying victims. Her parents are supportive. Her excellent school has a no-tolerance policy for cyberbullying. But neither the school nor the police could act until Alice could attach a name to her suspected cyberbully. This is not an easy task when senders mask their identities using an app or text service designed for that purpose.

The first step involved reference to **textem.net's terms of use**, which prohibit the sending of harassing or abusive texts from the site and caution potential anonymous texters that textem.net will assist victims of such practices by providing the Internet Protocol address and time stamp associated with the abusive text. As promised, textem.net provided both.

An IP address alone, however, is not enough. The Internet is full of so-called IP geolocation sites providing a general location of an IP address and the name of the Internet Service Provider, or ISP, for that address. Through the use of this type of geolocating website, we were able to narrow our search for the suspected IP address to one area of Los Angeles, served by a large cable Internet service provider.

Thus begins our adventures with Alice down this legal rabbit hole.

In dealing with the cable ISP, we encountered the first major roadblock—the **Cable Privacy Act**. This law prohibits disclosing "personally identifiable information" of cable subscribers to the average person without a court order and notice to the subscriber.

"Cyberbullies have all the tools they need to launch their attacks. Victims should have the tools they need to defend themselves."

Alice enters the world of the unknown. The most efficient method for obtaining a court order to restrain the perpetrator was to apply to the Los Angeles Superior Court's civil-harassment department—or so we thought. We were informed, however, that a court order or restraining order could only be issued against a known individual. 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 falls down the rabbit hole of litigation. We next sought a court order requiring the cable ISP to provide the identity of the subscriber associated with the IP address from which the anonymous text originated. The first judge was unsympathetic to our preteen'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, when young people seem to have smartphones appended to their heads.

Alice discovers another path. We served a subpoena on the cable ISP to produce the subscriber's name, which ordinarily would have the same effect as a court order in California. But not according to this cable ISP. They would have no problem responding to a court order, but refused to respond to a mere subpoena.

Alice goes back to court. We next appeared for a court order compelling the cable ISP to respond to the subpoena, a step that the service provider did not oppose. The court issued the order, required the provider to identify the subscriber after notifying them under terms of the Cable Privacy Act that their identity was being sought, also advising them of the 10-day period to object to the identity's being provided.

And then we waited. Finally, several months and tens of thousands of dollars later, we obtained the name of the perpetrator who sent the cyberbullying text.

With that information in hand, Alice's parents approached the school administrators, who initiated a dialogue with the parents of the cyberbullies. Not surprisingly, the identified classmates first denied having sent the offensive text, then pointed the finger at one another in an attempt to create reasonable doubt in the minds of the school administration. But the evidence was undeniable.

Alice was fortunate that her family was able to afford the lengthy and expensive process of identifying her tormentors. Not all victims have similar support. We need a better solution.

Our courts must have a speedier and more efficient way of obtaining identifying information in these cases. One solution would be to empower legal agencies such as Los Angeles' civil-harassment department to issue the needed order to Internet service providers when victims demonstrate good cause. This would reduce both costs and time, by not having to file a lawsuit, serve a subpoena that may be ignored, and seek a court order to fulfill a simple request for a name.

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 information from Internet service providers would remove the current barriers, bring cyberbullies into the light, and avoid others' having to follow in Alice's footsteps in their own adventures in Wonder-Who Land.

Kenneth A. Linzer is a partner at the Los Angeles law firm Linzer Law Group, PC, where he counsels executives, business owners, and boards of directors in matters including strategic planning and corporate governance.

Vol. 34, Issue 24, Pages 31, 36

Published in Print: **Alice in Wonder-Who Land**