

Why the Cyberbullying Prosecution Is A Bad Idea

The tragic case of Megan Meier has spawned an indictment that, if upheld by the federal courts, could turn every Internet “terms of service” violation into a potential felony. The expansive reading of a federal statute by Los Angeles-based United States Attorney Thomas P. O’Brien might signal the Ice Age of Internet expression. As sad as the Megan Meier story is, as much as every shred of decency in our instincts cries out for retribution against her tormentor, O’Brien’s gambit is not the answer. As a guardian of the law, he should guard against throwing the First Amendment onto the tracks for the sake of a politically popular prosecution.

The attorneys for the Defendant, Lori Drew, will probably challenge the May 15th indictment on the grounds that the facts, as alleged, do not provide the basis for a criminal prosecution. I think they would be right. This prosecution is likely to end with a whimper: dismissal on motion.

Most people are familiar with the back story. Megan Meier, a shy and somewhat troubled Missouri thirteen year-old, engaged in an Internet feud with a classmate, a former close friend. The friend’s mother, Lori Drew, was concerned about what she felt was cyberbullying on Megan’s part, and decided to teach Megan a lesson. As has been reported and was recited in the indictment, Drew compelled a nineteen year-old acquaintance to create a false identity on “MySpace” and lure Megan into an elaborate and remarkably cruel practical joke.

The false identity was that of “Josh Evans,” a fictional sixteen-year old boy who claimed to be attracted to Megan and lured her in with praise and suggestive come-ons. After Megan developed a crush on him, “Josh Evans” abruptly broke it off, and told her the world would be happier if she were dead. An hour later, Megan hanged herself. Lori Drew immediately ordered her acquaintance to terminate the MySpace account and eliminate all traces of “Josh Evans.”

In space, they can’t hear you scream. In cyberspace, a scream might be heard for eternity. All public evidence of “Josh Evans” was gone, but he lived on in the databank of a computer server in Los Angeles. Furthermore, there was evidence on the Meier’s home computer and, of course, in the memories of those closest to the events. Although Megan had a history of depression and other behavioral problems and was susceptible to low self-esteem, the inescapable suspicion was that Lori Drew’s cruel hoax pushed her over the edge to suicide.

State and federal law enforcement agencies investigated and found no basis for criminal charges. While Drew’s moral culpability was on display for all to judge, no criminal statute seemed to address the heinous impersonation and public humiliation that contributed in large part, if not totally, to the untimely and unnecessary death of Megan Meier. Then Mr. O’Brien got creative.

The primary statute that Drew is accused of violating is known as the “Computer Fraud and Abuse Act” (CFAA). The underlying legal and legislative history suggests that the Act was designed for hackers and those who unleash malicious programs on the Internet, like worms and viruses, as well as those who enter computers and unlawfully remove confidential data. The language of the Act reflects that view. Nonetheless, O’Brien has decided to stretch the CFAA into a large enough sack to contain the actions of Lori Drew. Unfortunately, everybody who acknowledges a “terms of service” agreement as a condition for accessing a web site would also fit. The legal term for such an ill-fitting sack is “overbreadth.”

The CFAA section used against Drew applies to whoever “intentionally accesses a computer without authorization or exceeds authorized access.” In Counts 2, 3, and 4 of the May 15th indictment, O’Brien alleges this unauthorized access: “In violation of MySpace TOS, accessed MySpace servers to obtain information regarding M.T.M.” (The initials refer to Megan Meier.) That’s it. No hacking. No false password. No tampering with code and no ruse to fool the machine. Just breaking a set of rules that Drew, like most Internet users, probably didn’t take the time to read.

A prescient article in the New York University Law Review, published in November, 2003, predicted the dangerous expansion of the CFAA that O'Brien is attempting to use against Lori Drew. "By using the law to aid sympathetic plaintiffs," wrote Orin S. Kerr, "the courts inadvertently have handed prosecutors a broad and powerful tool to punish breaches of contracts relating to computer use. Nearly any use of a computer that is against the interests of its owner is an 'access' to the computer either 'without authorization' or 'exceeding authorized access' under these precedents, triggering severe criminal penalties."

Kerr warned that, "broad judicial interpretations of unauthorized access statutes could potentially make millions of Americans criminally liable for the way they send e-mails and surf the Web."

Fortunately, Kerr also suggested a more reasonable interpretation of the statute that restricts it to the purposes originally intended. Kerr notes that unauthorized access can be "code based" or "contract based." The difference between the two is that code-based restrictions prevent the visitor from entering, while contract-based restrictions allow entry. Kerr argues that contract-based restrictions cannot satisfy the "unauthorized" element of the statute because they do, in fact, allow access. What they prohibit is remaining.

Examples: password protection is a code restriction. Unauthorized entry requires fooling the code. A terms of service agreement is a contractual restriction. Access is permitted, but maintaining access depends on complying with the terms of service agreement.

When the federal district court in Los Angeles weighs the inevitable motion to dismiss, the judge will first look to see if there is any precedent within the Ninth Circuit. The judge will find a new case, decided on February 20, 2008, that partly relied on the Kerr article.

The case is *Shamrock Foods Company vs. Jeff Gast, et. al.*, and the decision was handed down by the United States District Court for the District of Arizona. In the *Shamrock* case, an employee who took a position with another employer used his authorized access to Shamrock's computers to remove confidential data.

"Given the plain language, legislative history, and principles of statutory construction," wrote Judge Roslyn Silver, "the restrictive view of 'authorization' is adopted." The "restrictive view" was the code-based interpretation of Kerr, whom Silver cited with approval. Silver ruled that Gast violated a contractual provision, but was not denied access to the data, and did not gain "unauthorized access."

No matter how viscerally satisfying, the prosecution of Lori Drew endangers the free exchange of ideas on the Internet and kneecaps the First Amendment. Hopefully, the Court's sympathies will lie with the Amendment, no matter how popular the alternative might be.

© May 17, 2008 by Mike Tully