

TYPES NOT MAPPED YET August 23, 2022 | TTR not mapped yet | Mark Sableman

# Can Internet mischief be caught?

In addition to being the world's greatest communications medium, the Internet is one of the most effective conduits for fraud, illegality, and other mischief. Moreover, perpetrators, and the general public, tend to think that this kind of misconduct is uncatchable.

But Internet mischief may be more catchable than is generally assumed. And the tide of public indifference may have turned; law enforcement and aggrieved persons are becoming more aggressive at asserting their rights.

Consider some of the well-known pieces of Internet mischief (a term I'll use to encompass criminality, fraud, revenge, hate, and other intentionally harmful activities):

- The recent viral TikTok video providing how-to instructions for stealing certain Kia and Hyundai vehicles.
- Deliberate misinformation from domestic extremists, foreign governments, sophisticated fraudsters, or others.
- Revenge porn, in which a former intimate partner posts embarrassing photos or videos.
- Fake online reviews and targeted campaigns in which people hurt by business, legal, or personal affairs make hurtful posts directed at their perceived enemies.
- Common frauds, in which fake emails or websites are used to entice people to send money to the perpetrators.

There are so many new and different forms of Internet mischief that it has spawned a whole new lexicon – for example, doxing (publishing private information on the internet); swatting (falsely reporting crimes and sending law enforcement after innocent people), revenge porn (non-consensual intimate imagery distribution), phishing (sending fake emails to induce individuals to reveal personal information), cyber harassment, and cyber stalking.

A central concern with all of these activities is that they can be carried out covertly without traceability to the perpetrator, thus enabling the perpetrator to escape detection, responsibility, and sanction. Also, there seems to be a general feeling that Internet expression, no matter how harmful, evades legal accountability, perhaps because of the First Amendment, inadequacy of current laws, or social acceptance of extreme online expression.

In fact, however, neither our legal system nor our technological investigative capabilities are as impotent as are assumed.

Initially, the simple anonymity in which most Internet mischief-makers wrap themselves isn't invulnerable. They often sign up for web email using fake identities, and then use them or other fake IDs, and the email addresses, to register on social media. Those who are a bit more sophisticated may use virtual private networks to further hide themselves. Depending on the activity, torrents or other software designed to prevent traceability may be part of their scheme.

But shrewd investigators can often find the perpetrators despite these shields. I've subpoenaed web email providers, and service providers, to trace back fake email accounts to the original perpetrator. Special Counsel Robert Mueller was able to trace Russian election interference on the Internet back to 12 specific people operating out of two specific military units at two specific addresses in Moscow. He laid out their conduct in great detail in an [indictment](#).

Similarly, many revenge porn posters thought they had cleverly hidden their traces, but many successful revenge porn prosecutions and civil claims have identified, caught, and sanctioned perpetrators.

Then there's the difficulty of conducting any significant operation totally in Internet darkness. In one notable case, a fraudster took many precautions in setting up a magazine copyright infringement scheme, registering a domain name through a post office box in Antigua, and using servers in renegade foreign jurisdictions. But he was caught when a lawyer for the magazine industry found a trademark application he filed for his service.

Perhaps the biggest impediment to catching Internet mischief has been that many victims, and even some law enforcement agencies, have assumed that our laws don't reach this kind of mischief. But some gaps in the law have been filled (for example, hacking and revenge porn laws), and traditional legal tools can still reach much of this misconduct.

Take the viral TikTok video instructing on the stealing of cars. It's not protected speech, particularly in light of the 1997 *Rice v. Paladin Enterprises, Inc.* decision by the now-famous Fourth Circuit Judge J. Michael Luttig concerning the book "How to Hire a Hit Man." Judge Luttig's ruling held that "speech that constitutes criminal aiding and abetting does not enjoy the protection of the First Amendment." Law enforcement can, and should, find and prosecute the creators of the car stealing video. Victims of thefts that followed the video's instructions may even have civil claims. The recent successful victims' civil lawsuit against the organizers of the Charlottesville white supremacy rally, *Sines v. Kessler*, demonstrates that victims can seek recompense for harm deliberately set in motion through Internet exhortations to illegal conduct.

Civil lawsuits are being conducted against alleged misinformation providers. The prominent Dominion Voting System lawsuits against Fox News, Rudolph Giuliani, Sydney Powell and others; the similar Smartmatic lawsuits; and the case currently being brought by Georgia poll worker Ruby Freeman against Gateway Pundit, all assert claims, based on defamation and related laws, against speakers who they claim deliberately and knowingly made false and hurtful statements.

Misinformation that hurts society generally and not specific individuals probably can't be addressed civilly, and of course any prosecutions would need to be sensitive, to protect First Amendment protected expression. But if Mueller could identify specific Russians who were responsible for misinformation out of Moscow, surely law enforcement can identify and hold accountable the relatively unsophisticated Americans who have created misinformation campaigns far outside the bounds of legitimate discourse.

For years, Internet mischief makers acted as if they possessed a "Get out of jail free" card, because of their victims' fears about the difficulty of finding the perpetrators and bringing them to justice. But the tide may be turning, toward a greater willingness to investigate and prosecute.

## authorsTest

A dark gray rectangular placeholder for an author's photo, with the name 'mark' and 'Mark Sableman' written in white text below it.

mark

Mark Sableman