By Liam Hanlon, Jud Welle & Scott Nawrocki

January 6 and Beyond: Understanding the New Social Media Landscape

The storming of the US Capitol on January 6 shocked the nation and laid bare the dangerous consequences that online radicalization poses to American democracy. Attorney General Merrick Garland, in his Senate confirmation hearing on February 22, declared that domestic terrorism would be his "first priority." But the implications of the Capitol riot will be felt well beyond the Justice Department and the halls of Congress. Corporate America is also coming to grips with the gravity of potential threats emanating from obscure corners of the Internet, which can carry substantial risks to their operations and reputation.

Mainstream social media platforms, such as Facebook, Twitter, and YouTube, have gradually instituted policies to clamp down on violent and hate speech. This process accelerated following the January 6 attack as lawmakers, journalists, and the general public scrutinized websites that facilitated the planning, coordination, and livestreaming of the incursion. Twitter and Facebook banned, or "de-platformed," President Donald Trump. Twitter and Facebook also removed large swaths of users, with Twitter reportedly suspending more than seventy thousand accounts. Both companies increased their monitoring of far-right hashtags and groups on their platforms. Google and Apple swiftly banned Parler—a social media site popular with far-right extremists—from their app stores, and Amazon cut off hosting infrastructure to it.

However, monitoring and, where necessary, de-platforming this type of speech can create unintended consequences. As advocates of violent extremism of all types are pushed out of mainstream digital platforms, they often move to more marginal applications and websites that have emerged to fill the void. This presents a challenge for companies that want to make sure their employees, counterparties, brand ambassadors, and even clients aren't tainted by links to online extremist communities.

Recent news investigations have reported on the migration of extremist users to platforms like Gab, Parler, and MeWe, which tend to mimic Facebook and Twitter. Violent and racist chatter has also ballooned in the messaging apps Telegram and Signal, which are particularly opaque in their use of encrypted messaging and private messaging boards. Research firm App Annie reported that Telegram jumped from 110th to fifth in a list of most downloaded apps in the wake of the Capitol riot and Trump's

de-platforming. MeWe—which was not even listed in the top 1,000—moved to twelfth. Signal jumped from 750th to first.

Monitoring these new, less centralized platforms can be like a game of whack-a-mole. Websites crop up and then go dark, only to emerge on a different webhosting service. Parler has reemerged and is now hosted by another webservices company. The website TheDonald.win, which was used to plan the January 6 insurrection, was temporarily shut down before rebranding as Patriots.win.

Extremists also meet on the Dark Web, which is loosely defined as a collection of websites that are not indexed by search engines and are anonymous for its users. This part of the internet is most notoriously known as a marketplace for illicit goods, such as stolen information, black market drug sales, and child pornography.

The Implications for Your Organization

The new social media landscape has serious implications for organizations seeking visibility into extremist behavior that could threaten their business, people, and reputations. Locating and deciphering potential danger signs lurking on obscure social media platforms is now a critical element of risk management. With experienced and agile investigative support, you can spot these hazards before they taint your organization. We detail four scenarios below:

- **Due Diligence:** A company's reputation is one of its most valuable assets. Whether it is vetting a current or prospective board member or a business partner, you need to be aware of conduct and statements that are anathema to the organizational culture. Better to learn that your top CFO candidate posted a "Stop the Steal" hashtag on Parler from the US Capitol before you make the job offer than after.
- **Proxy Battles:** Proxy battles involve understanding both your own vulnerabilities and those of your adversary. The January 6 attack has added new urgency to transparency surrounding corporate political spending and lobbying. Surfacing intelligence that a director candidate participates in fringe social media activity can be used to defend against his nomination.
- **Active Threat Monitoring:** For better or worse, public actions by organizations are often filtered through political lenses. This can lead to fervent political supporters taking aim at a company and its employees for a perceived political injustice. In these instances, companies need to protect their brand and personnel. It is critical to understand the new social media landscape to understand where discussions are taking place and how to identify potential threats.
- **Cyber Threats:** Companies should ensure their information technology architecture monitors for high-risk social media platform activity and places these applications on their "deny list." While these applications were developed with user privacy in mind, security may not be incorporated into their application development lifecycle. This issue is even more difficult to navigate for organizations with a "Bring Your Own Device (BYOD)" policy. The risk of information leakage between work applications and unvetted applications on a BYOD presents challenges for information security personnel.

A Trained Eye to Help You Navigate This New Environment

Understanding the reach of this new social media environment may seem daunting, but an experienced and sophisticated investigative team can help navigate it and mitigate your risk. The key to many modern investigative techniques is combining the use of sophisticated database tools with experienced human analysis. It is no different with the rapidly changing social media landscape.

Social media analysis tools are slowly beginning to incorporate these new platforms into their search capabilities but are usually one step behind the curve. Many of these platforms are also purposefully constructed to limit the effectiveness of keyword searches in order to preserve anonymity and limit external monitoring. Here is how a well-trained human eye can play a decisive role:

- An experienced investigator will understand which message boards and groups are relevant to a specific investigation. Many of these are unsearchable or require approval to join by the group moderator.
- A social media analysis tool is typically driven by text searches. This may prove ineffective in the common situation of fringe groups that communicate primarily through images and memes. A seasoned investigative eye can review these images and decipher their meaning.
- New websites and messaging apps crop up or old ones become favorable again when de-platforming happens. An investigative team with knowledge of these shifting tides will be able to quickly tell you where the action is happening at a given moment.
- Extremist groups often speak in coded language in order to avoid detection from content moderators. A savvy investigator knows where fringe actors are conversing and what their language is like.
- Anonymity is often the most important quality for extremists seeking new platforms, but more often than not, their identify is not as well-guarded as they may think. Using open source research techniques, we can help attribute seemingly anonymous users to real actors.

Social media is changing, and not necessarily for the better. Rather than be caught off guard, firms should seek to get ahead of the next news cycle by taking steps to identify the hidden risks of an increasingly opaque and dangerous digital landscape.

Contact

Liam Hanlon
Associate Managing Director
+1 212 537 5300
lhanlon@nardelloandco.com

Scott Nawrocki
Managing Director, Digital Investigations & Cyber Defense
+1 212 537 5300
snawrocki@nardelloandco.com

Jud Welle
Managing Director, Head of Digital Investigations & Cyber Defense, and Chief Counsel, Cybersecurity & Privacy
+1 212 537 5300
jwelle@nardelloandco.com

Nardello WE FIND OUT & Co.