



January 2024

COUNTERING VIOLENT EXTREMISM

FBI and DHS Need Strategies and Goals for Sharing Threat Information with Social Media and Gaming Companies

Why GAO Did This Study

In recent years, content on social media and gaming platforms that promotes domestic violent extremism has influenced several high-profile attacks, according to experts and agency officials. As a result, some social media and gaming companies, as well as federal agencies, are making an effort to understand and address online content that promotes domestic violent extremism.

GAO was asked to review domestic violent extremists' use of social media and gaming platforms. This report (1) describes the purposes for which domestic violent extremists use these platforms; (2) describes how selected companies report mitigating content promoting domestic violent extremism; and (3) assesses the extent to which the FBI and DHS have developed goals and strategies for sharing threat-related information with companies.

GAO reviewed FBI and DHS documentation and interviewed officials. GAO obtained views from 16 subject matter experts identified by the National Academies of Sciences and prior work. GAO also interviewed representatives from a non-generalizable sample of five social media and gaming companies.

What GAO Recommends

GAO recommends that the FBI and DHS each develop strategies and goals for sharing information related to domestic violent extremism with social media and gaming companies. The agencies concurred with the recommendations.

View [GAO-24-106262](#). For more information, contact Triana McNeil at (202) 512-8777 or McNeilT@gao.gov.

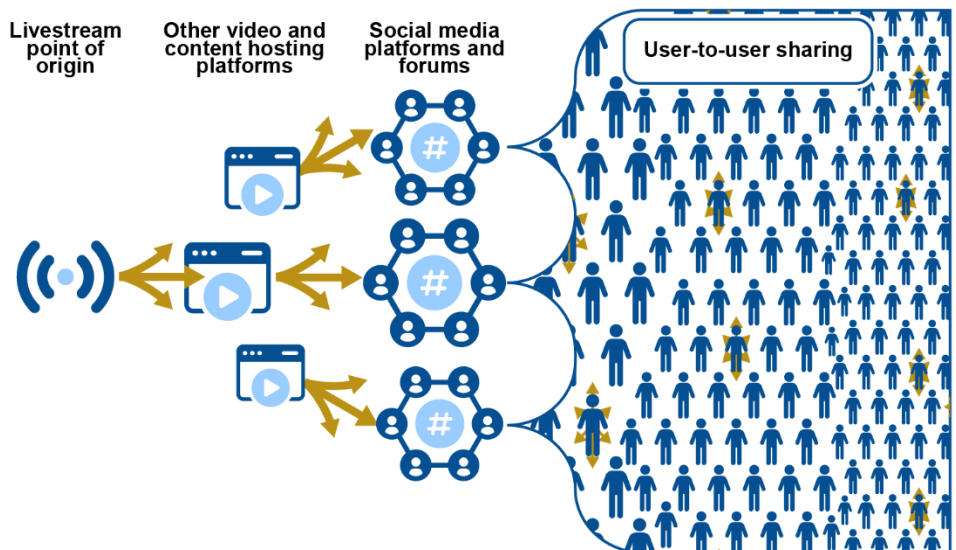
COUNTERING VIOLENT EXTREMISM

FBI and DHS Need Strategies and Goals for Sharing Threat Information with Social Media and Gaming Companies

What GAO Found

Domestic violent extremists use social media and gaming platforms for several purposes, including to reach wide audiences; to insert their extremist ideas into the mainstream; and to radicalize, recruit, and mobilize others, according to government reports and experts GAO spoke with (see figure). Experts noted that violent extremists generally use a variety of platforms for different purposes, depending on available features, audiences, and content moderation practices.

Example of the Viral Nature of Domestic Violent Extremists' Use of Online Platforms



Source: GAO analysis of U.S. Department of Homeland Security, FBI, and National Counterterrorism Center information; Icons-Studio/stock.adobe.com. | GAO-24-106262

According to social media and gaming companies GAO met with, they use various content moderation tools to identify and remove content they determine violates their platforms' policies related to domestic violent extremism on their platforms. For example, they report using machine learning tools to scan for content that violates their policies, as well as reviews by employees. However, companies and experts reported that several factors affect these moderation efforts, such as company financial considerations and diversity in standards of acceptable content. For example, content banned on one platform could be allowed on another.

The Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) have mechanisms to share and receive domestic violent extremism threat-related information with social media and gaming companies. However, neither agency has developed a strategy that articulates how it identifies and selects companies to engage with or the goals and desired outcomes of those engagements. Without a strategy or goals, the agencies may not be fully aware of how effective their communications are with companies, or how effectively their information-sharing mechanisms serve the agencies' overall missions.

Contents

Letter		1
	Background	5
	Domestic Violent Extremists Can Use Online Platforms to Radicalize, Recruit, and Mobilize Others	12
	Selected Companies Reported Using Various Tools to Mitigate Content that Promotes Domestic Violent Extremism	16
	The FBI and DHS Have Not Developed Strategies for Information-Sharing with Social Media and Gaming Companies	23
	Conclusions	30
	Recommendations for Executive Action	30
	Agency Comments	30
Appendix I	Experts Who Participated in GAO’s Interviews and Relevant Affiliations	32
Appendix II	FBI and DHS Views Related to their Efforts to Address Online Content Promoting Domestic Violent Extremism	33
Appendix III	Efforts to Prevent and Counter Violent Extremism on Online Platforms	34
Appendix IV	Comments from the Department of Homeland Security	36
Appendix V	GAO Contact and Staff Acknowledgments	39
Table		
	Table 1: Experts Who Participated in GAO’s Interviews and Relevant Affiliations	32
Figures		
	Figure 1: Summaries of FBI and DHS Domestic Terrorism Threat Categories	7

Figure 2: Ways that Domestic Violent Extremists Use Online Platforms	13
Figure 3: Recruitment Stages of Some Violent Extremists on Social Media Platforms	14
Figure 4: Content Moderation Policies and Tools that Companies May Use	17
Figure 5: Example of the Viral Nature of Domestic Violent Extremists' Use of Online Platforms	23
Figure 6: Examples of FBI and DHS Mechanisms for Sharing Domestic Violent Extremism Information with Social Media and Gaming Companies	24

Abbreviations

DHS	Department of Homeland Security
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
I&A	Office of Intelligence and Analysis
NASEM	National Academies of Sciences, Engineering, and Medicine
NCTC	National Counterterrorism Center

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



January 31, 2024

The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Seth Magaziner
Ranking Member
Subcommittee on Counterterrorism, Law Enforcement, and Intelligence
Committee on Homeland Security
House of Representatives

Domestic violent extremists have used online platforms to recruit followers, plan and rally support for in-person actions, and disseminate materials that contribute to radicalization and mobilization to violence, among other purposes.¹ In June 2023, the Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) identified lone offenders and small groups of individuals—both of whom are often radicalized online—who commit acts of violence that are motivated by a mix of ideological, socio-political, and personal grievances as one of the most significant terrorism threats.² In January 2022, Department of Justice (DOJ) officials testified at a congressional hearing that investigations of suspected domestic violent extremists more than doubled since the spring of 2020.³

Social media and gaming platforms are ever present in the lives of many Americans. In 2021, about 72 percent of Americans reported using social media, up from 50 percent in 2011.⁴ Further, in 2023, the Entertainment Software Association found that about 65 percent of Americans reported

¹Department of Homeland Security, Office of Intelligence and Analysis, *Homeland Threat Assessment 2024* (2023).

²Federal Bureau of Investigation and Department of Homeland Security, *Strategic Intelligence Assessment and Data on Domestic Terrorism* (Washington, D.C.: June 2023).

³*The Domestic Terrorism Threat One Year After January 6, Before the S. Comm. On Judiciary*, 117th Cong. (2022). (statement of Matthew G. Olsen, Assistant Attorney General, Department of Justice; and Jill Sanborn, Executive Assistant Director, National Security Branch, Federal Bureau of Investigation).

⁴Pew Research Center, *Social Media Fact Sheet* (Apr. 7, 2021).

playing video games.⁵ While social media and gaming platforms are integral to modern life, content shared on these platforms has also influenced mass attacks by violent extremists. The U.S. Secret Service found that 23 percent of mass attack perpetrators from 2016 through 2020 posted concerning communications online, such as threats to harm others and referencing previous mass shootings or hate toward a particular ethnic group.⁶ In addition, a 2022 report by the Anti-Defamation League found that 20 percent of adult gamers and 15 percent of young gamers reported being exposed to white supremacist ideologies in online games.⁷

The FBI, within DOJ, and DHS are the main federal agencies charged with preventing terrorist attacks in the U.S., including attacks conducted by domestic violent extremists. With respect to information sharing and analysis, the FBI conducts investigative activities, and DHS conducts open source collection and analytical activities related to domestic violent extremist content posted online.⁸

You asked us to examine domestic violent extremists' use of social media and gaming platforms. This report (1) describes the purposes for which domestic violent extremists use social media and gaming platforms; (2) describes how social media and gaming companies report mitigating online content that promotes domestic violent extremism; and (3) assesses the extent to which the FBI and DHS have developed goals and strategies for sharing information on the threat of domestic violent extremists with social media and gaming companies.

To address our first and second objectives, we worked with the National Academies of Sciences, Engineering, and Medicine (NASEM) to identify and interview a nongeneralizable selection of experts in this subject matter area. We solicited recommendations from NASEM and identified

⁵Entertainment Software Association, *Essential Facts about the U.S. Video Game Industry* (July 2023).

⁶U.S. Secret Service, *Mass Attacks in Public Spaces: 2016-2020* (Jan. 2023).

⁷Anti-Defamation League, *Hate Is No Game: Hate and Harassment in Online Games 2022* (Dec. 2022).

⁸By statute, the Attorney General has primary investigative responsibility for all federal crimes of terrorism, and the FBI exercises lead agency responsibility on the Attorney General's behalf. 18 U.S.C. § 2332b(f); see also 28 C.F.R. § 0.85(l). The Homeland Security Act of 2002 established one of DHS's primary missions as preventing terrorist attacks within the U.S. Pub. L. No. 107-296, Tit. I, § 101(b)(1)(A), 116 Stat. 2135, 2142 (codified at 6 U.S.C. § 111(b)(1)(A)).

additional experts based on prior GAO work and expert recommendations. We selected 16 experts with relevant research or industry experience representing a range of perspectives related to domestic violent extremism. In particular, we selected experts from research organizations, advocacy organizations, and academic institutions with expertise on how domestic violent extremists use online platforms, and actions that technology companies have taken to address domestic violent extremist content. See appendix I for a list of the experts who participated in our interviews.

To help identify any potential biases or conflicts of interest, the eight experts that NASEM selected disclosed to us whether they had investments, sources of earned income, organizational positions, relationships, or other circumstances that could affect, or be viewed to affect their perspectives. None of the experts reported potential conflicts that would affect their ability to participate in the interviews. We then conducted semi-structured interviews with the 16 experts and analyzed the information obtained to identify the prevalence of common themes from the interviews.

To further describe how social media and gaming companies mitigate online content that promotes domestic violent extremism, we reviewed information and interviewed officials from a nongeneralizable sample of companies that operate social media and gaming platforms. To identify which companies to include, we reviewed articles and reports from academic literature, nongovernmental organizations, and the media published from January 2021 through January 2023 describing content promoting domestic violent extremism on the internet.

To identify articles and reports to review, we conducted searches using terms related to domestic violent extremism (such as “domestic violent extremism,” “domestic terrorism,” “mass shooting”) as well as terms related to online platforms (such as “social media,” “forum,” and “gaming”). We then counted the number of times various social media and gaming platforms were mentioned in the articles and reports. We selected the 10 companies whose platforms were cited the most. These platforms covered a range of different services, such as communication and messaging, forums, gaming, and social media. We then reviewed publicly available information for the 10 companies and reached out to all 10 companies for more information.

Of the 10 companies, five responded that they were willing to participate, and we then interviewed and requested information from these

companies.⁹ We used these interviews and public information to understand companies' terms of service, content moderation tools, and strategies related to mitigating content promoting domestic violent extremism, as well as any challenges they face in enforcing their policies.¹⁰ Of the five companies we interviewed, one operated a social media platform, one operated a forum platform, one operated a messaging platform, and two operated gaming platforms.

To address our third objective on the extent to which the FBI and DHS developed strategies for sharing information with social media and gaming companies, we reviewed FBI and DHS documentation and interviewed agency officials about the extent to which they have done so. We also asked the five companies we interviewed about federal efforts and information-sharing mechanisms related to domestic violent extremist content online. Additionally, we interviewed officials with the National Fusion Center Association and two fusion centers in proximity to social media and gaming companies to obtain additional context about the landscape of violent extremism online and their coordination efforts with DHS and the FBI.¹¹ We compared the FBI's and DHS's efforts against the principles and practices for documentation, goal setting, and strategizing in *Standards for Internal Control in the Federal Government* and *Evidence-Based Policymaking: Practices to Help Manage and Assess the Results of Federal Efforts*.¹²

We conducted this performance audit from September 2022 to January 2024, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe

⁹The companies we interviewed were Discord, Reddit, and Roblox, as well as a social media company and a game publisher that preferred to remain anonymous.

¹⁰In addition, we visited a social media company as part of a related engagement to observe a demonstration of their content moderation tools and gather additional context.

¹¹Fusion centers are state or locally run centers that serve as a focal point for intelligence gathering, analysis, and sharing of threat information among federal, state, and local partners.

¹²GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014); GAO, *Evidence-Based Policymaking: Practices to Help Manage and Assess the Results of Federal Efforts*, [GAO-23-105460](#) (Washington, D.C.: July 12, 2023).

that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Definition of Domestic Violent Extremism and Threat Group Categories

According to the FBI and DHS, a domestic violent extremist is an individual based and operating primarily within the U.S. or its territories without direction or inspiration from a foreign terrorist group or foreign power, who seeks to further political or social goals through unlawful acts of force or violence dangerous to human life.¹³ For the purposes of this report, we use the term “content promoting domestic violent extremism” to generally refer to any text, graphic, video, audio content, or other communication made on social media or gaming platforms, that supports or encourages the use of violence to further a political or social goal in the U.S.

There is no federal statute that specifically criminalizes domestic violent extremism. However, individuals who plan or carry out violent extremist attacks may be federally prosecuted under a wide range of criminal statutes corresponding to their conduct. For example, federal prosecutors can charge firearms violations, interstate threats, or hate crimes when applicable.

Content promoting domestic violent extremism is, on its own, not necessarily subject to criminal penalties because it may be

¹³According to the FBI and DHS, the terms “domestic violent extremism” and “domestic terrorism” are used interchangeably. Within DHS, the Office of Intelligence and Analysis defines domestic terrorism as “terrorism that is not international terrorism.” Domestic terrorism is defined in statute as activities that occur primarily within the territorial jurisdiction of the U.S.; involve acts dangerous to human life that are a violation of the criminal laws of the U.S. or of any state; and appear to be intended to: intimidate or coerce a civilian population; influence the policy of a government by intimidation or coercion; or affect the conduct of a government by mass destruction, assassination, or kidnapping. 18 U.S.C. § 2331(5). The FBI uses this definition. DHS relies on a similar definition of terrorism under the Homeland Security Act of 2002. Pub. L. No. 107-296, Tit. I, § 2(15), 116 Stat. 2135, 40 (codified at 6 U.S.C. § 101(18)). The Homeland Security Act definition applies to two categories of acts: (1) those dangerous to human life and (2) those potentially destructive of critical infrastructure or key resources. According to DHS officials, DHS considers acts that are potentially destructive of critical infrastructure to be acts that are dangerous to human life for purposes of the definition of “domestic violent extremism.”

constitutionally protected under the First Amendment.¹⁴ The First Amendment protects a broad range of speech and expression, even if such speech may be considered unsavory or offensive. According to the FBI and DHS's *Strategic Intelligence Assessment and Data on Domestic Terrorism*, the mere advocacy of political or social positions, political activism, use of strong rhetoric, or generalized philosophic embrace of violent tactics does not constitute violent extremism and is constitutionally protected.¹⁵

Alternatively, there may be circumstances in which speech loses constitutional protection and constitutes a crime itself if the speech, for example, breaches the threshold of a "true threat." A true threat—speech that represents a threat made with the intent of placing a person or group in fear of bodily harm or death—is not necessarily protected under the First Amendment.¹⁶

In a 2023 report, the FBI and DHS jointly identified five domestic terrorism threat group categories the U.S. Government has used since 2019.¹⁷ These categories include violent extremism motivated by (1) race or ethnicity; (2) anti-government or anti-authority sentiment; (3) animal rights or environmental sentiment; (4) abortion-related issues; and (5) other domestic terrorism threats not otherwise defined or primarily motivated by the other categories. See figure 1 for additional information. The report noted that domestic violent extremists can fit within one or multiple categories of ideological motivation and can span a broad range of groups or movements. According to the report, these categories help the

¹⁴The First Amendment states that Congress shall make no law abridging the freedom of speech. U.S. CONST. amend. I.

¹⁵Federal Bureau of Investigation and Department of Homeland Security, *Strategic Intelligence Assessment and Data on Domestic Terrorism* (June 2023).

¹⁶See *Chaplinsky v. State of New Hampshire*, 315 U.S. 568, 571 (1942) (noting that "it is well understood that the right of free speech is not absolute at all times and under all circumstances"); *Virginia v. Black*, 538 U.S. 343, 359 (2003) (holding that true threats "encompass those statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals"); *Counterman v. Colorado*, 600 U.S. 66 (2023) (holding that, in true-threat cases using online communications, the State must prove that the defendant had some subjective understanding of their statements' threatening nature).

¹⁷Federal Bureau of Investigation and Department of Homeland Security, *Strategic Intelligence Assessment and Data on Domestic Terrorism* (June 2023).

agencies better understand threats associated with domestic violent extremism.¹⁸

Figure 1: Summaries of FBI and DHS Domestic Terrorism Threat Categories



Source: FBI and U.S. Department of Homeland Security information; Icons-Studio/stock.adobe.com (illustrations). | GAO-24-106262

¹⁸In the report, FBI and DHS said domestic terrorism-related criminal actors' motivations vary, are nuanced, and sometimes are derived from a blend of categories. Federal Bureau of Investigation and Department of Homeland Security, *Strategic Intelligence Assessment and Data on Domestic Terrorism* (June 2023).

Federal Agency Roles and Responsibilities Related to Domestic Violent Extremism

The FBI and DHS are the primary federal agencies responsible for preventing violent extremist attacks in the U.S.¹⁹ The distinct missions of the FBI and DHS result in different roles and activities related to online content that promotes domestic violent extremism.²⁰

FBI. The FBI is the lead agency responsible for federal terrorism investigations and domestic intelligence efforts involving terrorist activities or acts in preparation for terrorist activities in the U.S.²¹ The FBI may conduct varying levels of assessments and investigations with an authorized purpose.²² As relevant, FBI investigations may include gathering online content.

The FBI uses various online services and resources, including commercially available open source analysis software, to support

¹⁹See 18 U.S.C. § 2332b(f) (noting “the Attorney General shall have primary investigative responsibility for all Federal crimes of terrorism); 28 C.F.R. § 0.85(l) (noting the FBI may “[e]xercise Lead Agency responsibility in investigating all crimes for which it has primary or concurrent jurisdiction and which involve terrorist activities or acts in preparation of terrorist activities within the statutory jurisdiction of the United States’); 6 U.S.C. § 111(b)(1)(A) (noting one of the primary missions of DHS is to prevent terrorist attacks within the United States). See also Federal Bureau of Investigation and Department of Homeland Security, *Strategic Intelligence Assessment and Data on Domestic Terrorism* (June 2023).

²⁰In February 2023, we recommended that DHS and the FBI assess existing formal agreements to determine if they fully articulate a joint process for working together to counter domestic terrorism threats and sharing relevant domestic terrorism-related information. Both agencies agreed with the recommendations. The recommendations have not been addressed yet. See GAO, *Domestic Terrorism: Further Actions Needed to Strengthen FBI and DHS Collaboration to Counter Threats*, [GAO-23-104720](#) (Washington, D.C.: Feb. 22, 2023). According to DHS officials, in March 2023, I&A and FBI senior leadership met to discuss potential access by I&A to the FBI’s investigative files. I&A and the FBI continue to assess existing agreements. DHS officials reported that the FBI has solicited its workforce for a candidate to serve on rotation at I&A, to provide an additional on-site FBI resource at DHS with access to this information while discussions continue.

²¹18 U.S.C. § 2332b(f); 28 C.F.R. § 0.85(l).

²²According to the FBI’s Domestic Investigations and Operations Guide, an authorized purpose must be an authorized national security, criminal, or foreign intelligence collection purpose. However, simply stating such a purpose is not sufficient and the authorized purpose must be well-founded and well-documented. Further, FBI policies require all investigative and information gathering activities to be carried out in a manner consistent with the Constitution and the laws of the United States. In addition, these policies require the least intrusive means and methods to be considered by FBI personnel and—if reasonable based on the circumstances of the investigation—used in lieu of a more intrusive method.

investigations by searching publicly available online information, according to the agency.

DHS. DHS gathers, analyzes, produces, and shares information on emerging terrorist threats. DHS also develops resources and tools to build stakeholder capacity to reduce risk and increase resilience, according to officials. Within DHS, the Office of Intelligence and Analysis (I&A) is the primary office focused on gathering, analyzing, producing, and sharing information on emerging terrorist threats with federal, state, and local governments and private entities.²³ I&A personnel are authorized to collect publicly available information on U.S. persons, including public information on online platforms.²⁴ According to agency officials, this can include creation of a general social media account, such as a Facebook or X (formerly Twitter) account, to view public pages and groups. However, I&A analysts cannot interact with any individuals on the platforms. They also may not gather information from groups or chat rooms that require a login or a password.

The FBI and DHS provided views on their efforts to address online content promoting domestic violent extremism, which we describe in appendix II.

Agency legal considerations. In pursuit of their missions, the FBI and I&A may review publicly available online content, including content promoting domestic violent extremism, in certain circumstances as appropriate. According to agency policy, the FBI's investigative or intelligence activities may include collecting online content, including content promoting domestic violent extremism, that may otherwise be protected by the First Amendment, if it has a nexus to criminal activity or threats to national security. However, FBI investigative activities may not

²³See generally 6 U.S.C. § 121.

²⁴I&A's Official Usage of Publicly Available Information policy, and Intelligence Oversight Guidelines, define publicly available information as unclassified information that has been published or broadcasted in some manner to the general public, is available to the public by subscription or purchase, could lawfully be seen or heard by a casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public. Social media sites, internet sites, chat rooms, bulletin boards, and other electronic and other fora belonging to individuals or groups that limit access by use of criteria that cannot generally be satisfied by members of the public are not publicly available sources.

be conducted based solely on First Amendment activity.²⁵ In addition, I&A officials told us they may collect publicly available information that is protected by the First Amendment where it advances a national or departmental mission to do so, and where the collection is not for the sole purpose of monitoring protected speech or the lawful exercise of other legal rights.²⁶ According to I&A policy, I&A may not collect information for the purpose of affecting the political process in the U.S., for the purpose of retaliating against a whistleblower, or for the purpose of suppressing or burdening criticism or dissent.²⁷

Agency coordination. The FBI and DHS also work with other entities within the federal government, such as the National Counterterrorism Center (NCTC), to receive and share information. Within the Office of the Director of National Intelligence, NCTC has limited its work to the transnational and international dimensions of terrorist threats as of December 2022 in response to congressional direction, according to a

²⁵Federal Bureau of Investigation, *FBI's Domestic Investigations and Operations Guide* (Washington, D.C.; Sept. 17, 2021); Department of Justice, *The Attorney General's Guidelines for Domestic FBI Operations* (Washington, D.C.; Sept. 9, 2008); see also 5 U.S.C. § 552a(e).

²⁶According to I&A policy, collection is defined as obtaining or acquiring information from outside the Intelligence Community by any means, including, but not limited to, information that is volunteered, and regardless of whether the information is temporarily or permanently retained. Information that only momentarily passes through an I&A computer system is not collected. Collection is distinct from access to information in that collection requires that the information be copied, saved, or used in some manner, including, but not limited to, information that is copied or saved in the form of summaries, reports, or notes, whereas information that is accessed is merely viewed or examined, but is not collected even if it is transmitted on an I&A information technology system. Department of Homeland Security, Office of Intelligence and Analysis, *IA-900 Official Usage of Publicly Available Information* (Washington, D.C.: January 11, 2017); Department of Homeland Security, Office of Intelligence and Analysis, *IA-1000 Intelligence Oversight Program and Guidelines* (Washington, D.C.: January 19, 2017). In addition to agency policies, the Privacy Act of 1974 prohibits agencies from maintaining information about how U.S. citizens and lawful permanent residents exercise their First Amendment rights. A law enforcement exception authorizes agencies to maintain information about an individual's First Amendment activities if "pertinent to and within the scope of an authorized law enforcement activity." 5 U.S.C. § 552a(e)(7). According to I&A officials, I&A construes the term "law enforcement activity" as including the intelligence activities of I&A.

²⁷Department of Homeland Security, Office of Intelligence and Analysis, *IA-1000 Intelligence Oversight Program and Guidelines* (Washington, D.C.: January 19, 2017).

report authored by the FBI and DHS in coordination with NCTC.²⁸ For example, although DHS, FBI, and NCTC jointly produced a series of domestic violent extremism-focused intelligence products in 2022, consistent with congressional direction, NCTC is limiting its contribution to these products to analysis concerning domestic terrorism threats with an identified foreign nexus. However, NCTC also conducts strategic planning for counterterrorism activities within and among agencies and ensures that agencies have access to and receive the intelligence needed to accomplish their assigned activities.²⁹ NCTC is the primary organization responsible for “analyzing and integrating” all intelligence related to terrorism and counterterrorism, except for intelligence that pertains exclusively to domestic terrorism.³⁰ Although NCTC’s activities are focused primarily on transnational and international counterterrorism, it is authorized to receive domestic counterterrorism intelligence from other sources, such as I&A, which has a statutory duty to support NCTC’s mission.³¹

Social Media and Gaming Companies and Their Legal Considerations

We use the term “social media and gaming platforms” to describe a variety of platforms, with features that may include video streaming, profiles, groups, group messaging, discussion boards, online games, voice chat, and game distribution marketplaces. Some of these platforms allow users to “like” content or share it within or across platforms, allowing content to reach large audiences in a short amount of time. In addition, some social media platforms use recommendation algorithms to learn about users and deliver content to them based on their interests. Other

²⁸Department of Homeland Security and Federal Bureau of Investigation, *Strategic Intelligence Assessment and Data on Domestic Terrorism* (Washington, D.C.: June 2023). The DHS and FBI joint Strategic Intelligence Assessment cites congressional direction that NCTC limit production of intelligence products concerning terrorism threats in the United States absent an identified foreign nexus. NCTC has collaborated with the FBI and DHS on products that communicate updated threat information and assessments to federal, state, local, tribal, and private sector partners; the DHS and FBI joint Strategic Intelligence Assessment notes NCTC’s support to the FBI and DHS focuses on transnational threats and trends, and when assessing individual actors to identify any connections to international or transnational terrorism.

²⁹50 U.S.C. § 3056(d)(2),(5).

³⁰50 U.S.C. § 3056(d)(1).

³¹U.S.C. § 121(d)(1); 50 U.S.C. § 3056(e)(1) (noting that NCTC “may... receive intelligence pertaining exclusively to domestic counterterrorism from any Federal, State, or local government or other source necessary to fulfill its responsibilities and retain and disseminate such intelligence.”).

platforms provide opportunities for users to interact virtually while playing games.

As private companies, social media and gaming companies are not ordinarily constrained by the First Amendment and constitutional free speech considerations.³² Therefore, private companies can generally regulate content on their platforms according to their individually determined policies and user agreements. These policies may prohibit various types of conduct or content, potentially including content promoting domestic violent extremism.

Social media and gaming companies may have differing definitions of domestic violent extremist content based on their terms of service. We previously reported on company policies and data related to online hate speech and violent extremism.³³ Regardless of an individual platform's terms of service, platforms are generally shielded from liability for user-generated content. Section 230 of the Telecommunications Act of 1996, referred to as the Communications Decency Act, generally provides that interactive computer services providers, such as social media and gaming companies, are not treated as publishers and are therefore granted protection against legal action related to user-generated content on the platform.³⁴ For example, a social media company cannot generally be held liable for a threat that a user posts on its platform and proceeds to carry out.

Domestic Violent Extremists Can Use Online Platforms to Radicalize, Recruit, and Mobilize Others

According to experts and federal agencies, domestic violent extremists use online platforms to reach wide audiences; to insert their ideas into the

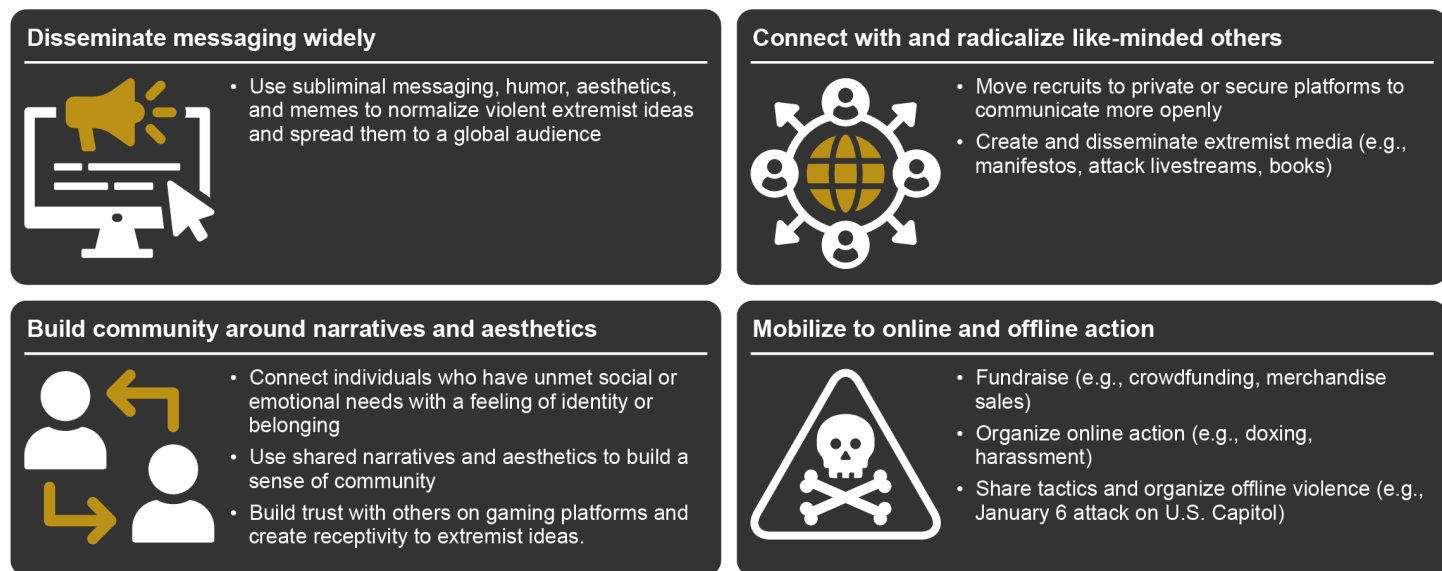
³²*Manhattan Cmty. Access Corp v. Halleck*, 139 S. Ct. 1921, 1930 (2019) (“[W]hen a private entity provides a forum for speech, the private entity is not ordinarily constrained by the First Amendment because the private entity is not a state actor. The private entity may thus exercise editorial discretion over the speech and speakers in the forum.”).

³³GAO, *Online Extremism: More Complete Information Needed about Hate Crimes that Occur on the Internet*, [GAO-24-105553](#) (Washington, D.C.: Jan. 2024).

³⁴Pub. L. No. 104-104, § 509, 110 Stat. 56, 138-139 (codified at 47 U.S.C. § 230).

mainstream; and to radicalize, recruit, and mobilize others (see figure 2).³⁵

Figure 2: Ways that Domestic Violent Extremists Use Online Platforms



Source: GAO analysis of information from expert interviews; Icons-Studio/stock.adobe.com (illustrations). | GAO-24-106262

Note: Doxing refers to the act of publicly identifying or publishing private information about someone, particularly as a form of punishment or revenge.

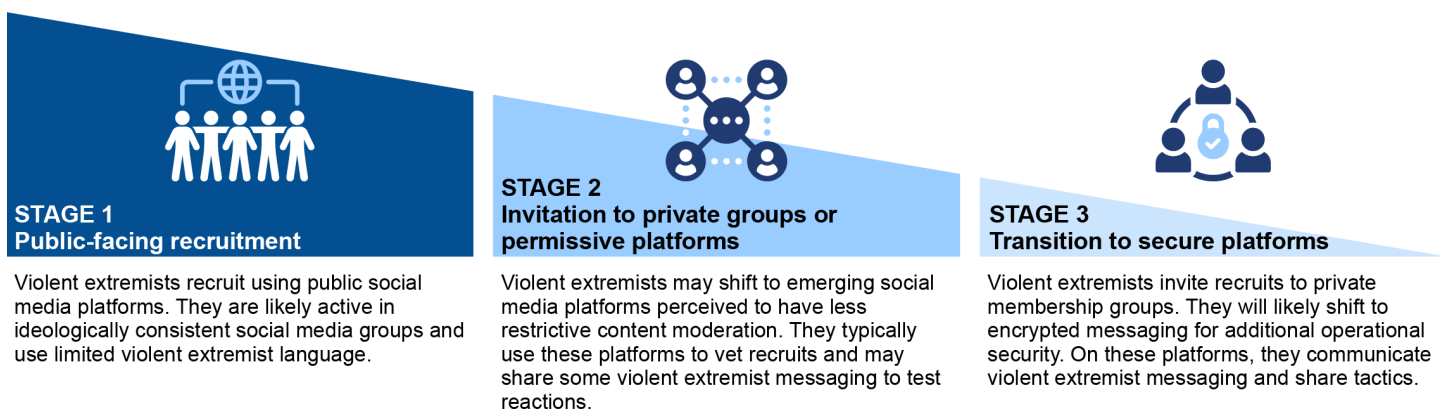
Like many internet users, domestic violent extremists use different platforms for different purposes. Social media and gaming platforms have varying features, which drive users' options and choices when using each platform. Similarly, domestic violent extremists use different tactics on social media and gaming platforms, depending on the features and audiences of each platform, as described below.

Large, public-facing social media platforms. Some domestic violent extremists use popular public-facing social media platforms with large user bases, such as Facebook and X, to radicalize others and spread watered-down versions of their ideology, particularly in like-minded groups, according to experts with whom we spoke. Violent extremists

³⁵Experts, and social media and gaming companies, may use definitions of domestic violent extremism that differ from the definitions FBI and DHS use.

may operate on multiple platforms, using less violent rhetoric on the large, public-facing platforms that are more likely to have and enforce content moderation policies, experts said. For example, one expert cited the example of a prominent neo-Nazi leader, who used less extreme humor on large, public-facing platforms to attract new followers and then displayed more extreme views on smaller platforms. Similarly, some violent extremists begin their recruitment on large, public-facing platforms, before transitioning recruits to increasingly private platforms where they can communicate more openly, according to I&A officials. The officials further said that several types of violent extremists, such as some militia violent extremists and racially and ethnically motivated violent extremists, use the same recruitment strategy (see figure 3).³⁶

Figure 3: Recruitment Stages of Some Violent Extremists on Social Media Platforms



Source: U.S. Department of Homeland Security information; Icons-Studio/stock.adobe.com (icons). | GAO-24-106262

Note: This figure and its source report focused on social media platforms and did not include gaming platforms. While domestic violent extremists' recruitment strategies work across platforms, the specific tools and methods used may vary by platform and platform type. See Department of Homeland Security, Office of Intelligence and Analysis, *Militia Violent Extremists Developing Online Networks Despite Content Removal Efforts*.

Some experts also told us that some violent extremists leverage the characteristics and features of large public-facing platforms, such as their recommendation algorithms and large user bases, to organically grow communities based on extremist narratives. For example, in 2020, the anti-government extremist movement known as Boogaloo surfaced on Facebook and grew in part based on Facebook's algorithm

³⁶Department of Homeland Security, Office of Intelligence and Analysis, *Militia Violent Extremists Developing Online Networks Despite Content Removal Efforts*.

Mass Shooting in Buffalo, New York

In May 2022, an alleged racially motivated violent extremist (RMVE) attacked a grocery store in Buffalo, New York, killing 10 individuals. The RMVE adhered to a white supremacist ideology—specifically targeting Black people—and drew inspiration from previous RMVE extremist attackers and their online materials.

The RMVE livestreamed his attack on a video streaming platform, replicating the visual style of a first-person shooter game. A recording of the attack as well as the attacker's manifesto—in which he documented his tactics and techniques to create a "how-to" guide for future attackers—quickly proliferated across the internet, despite the efforts of some companies to remove the content. Federal agencies assess that the existence of these materials online may inspire and enhance the capabilities of future attackers. The defendant pleaded guilty, was sentenced in state court, and is awaiting trial on federal hate crimes and other charges.

Source: Information from Federal Bureau of Investigation, National Counterterrorism Center, and U.S. Department of Homeland Security. | GAO-24-106262

recommending Boogaloo-related groups and merchandise to users with various ideologies, according to some experts.³⁷ According to experts, after a Boogaloo adherent killed a federal law enforcement officer in California, Facebook removed the groups.³⁸

Audience-specific social media platforms. Most experts told us that violent extremists use platforms with less restrictive policies to build a culture and narrative around their worldview that can draw in users looking for an identity and a community. For example, they may test new ideas and memes on these smaller platforms, and then users may repost the most well-received content on larger platforms. In addition, I&A officials told us that since the Capitol attack on January 6, 2021, violent extremists have increasingly started their recruitment efforts on secure communication platforms, such as encrypted messaging platforms, to evade law enforcement detection. We previously reported on federal agencies' use of online information related to the Capitol attack.³⁹

Online gaming platforms. Some experts we spoke with explained that violent extremists use online gaming platforms to engage with and befriend other gamers.⁴⁰ In particular, they said this strategy builds trust and social bonds in a gameplay setting and makes it easier to spread their ideas. For example, gamers may meet while playing together online and then use gaming-adjacent messaging platforms where gamers often gather socially to further connect and build communities around shared interests and social connection. In this way, these platforms can also provide a social space for violent extremist content to spread. This is consistent with an I&A report that said some domestic violent extremists

³⁷According to DOJ, the Boogaloo movement is a loosely organized anti-government extremist movement whose adherents believe there will be a civil war or uprising against the U.S. government following perceived incursions on constitutional rights—including the Second Amendment's right to bear arms—or other perceived government overreach. U.S. Attorney's Office, *Pasadena Man Who Allegedly Adheres to Extremist Anti-Government Ideology Charged in Federal Complaint with Possessing Machine Gun* (Jan. 26, 2023).

³⁸U.S. Attorney's Office for the Northern District of California, *Steven Carrillo Sentenced to 41 Years in Prison for Murder and Attempted Murder for Role in Drive-By Shooting at Federal Courthouse in Oakland*, (San Francisco, CA: June 3, 2022).

³⁹GAO, *Capitol Attack: Federal Agencies' Use of Open Source Data and Related Threat Products Prior to January 6, 2021*, [GAO-22-105963](#) (Washington, D.C.: May 2, 2022).

⁴⁰In addition to experts we spoke with, Intelligence Community reporting also identified violent extremists' use of gaming platforms. See National Counterterrorism Center, Department of Homeland Security, and Federal Bureau of Investigation, *Terrorist Exploitation of Online Gaming Platforms* (Oct. 24, 2023).

choose to use gaming-adjacent platforms for this purpose because they believe such platforms to be permissive of their content.⁴¹

One expert noted that there is no evidence directly linking violence in video games to real-world violence. However, another expert said violent extremists may selectively use video games with audiences they believe will be more receptive to violent extremist information. In addition, some violent extremists make and disseminate their own games that glorify or normalize past violent extremist incidents, such as re-creations of prior mass shootings. However, two experts said these games are not frequently used as a recruiting tool because they do not appeal to a wider audience, and it is easier for violent extremists to connect with others on messaging platforms instead.

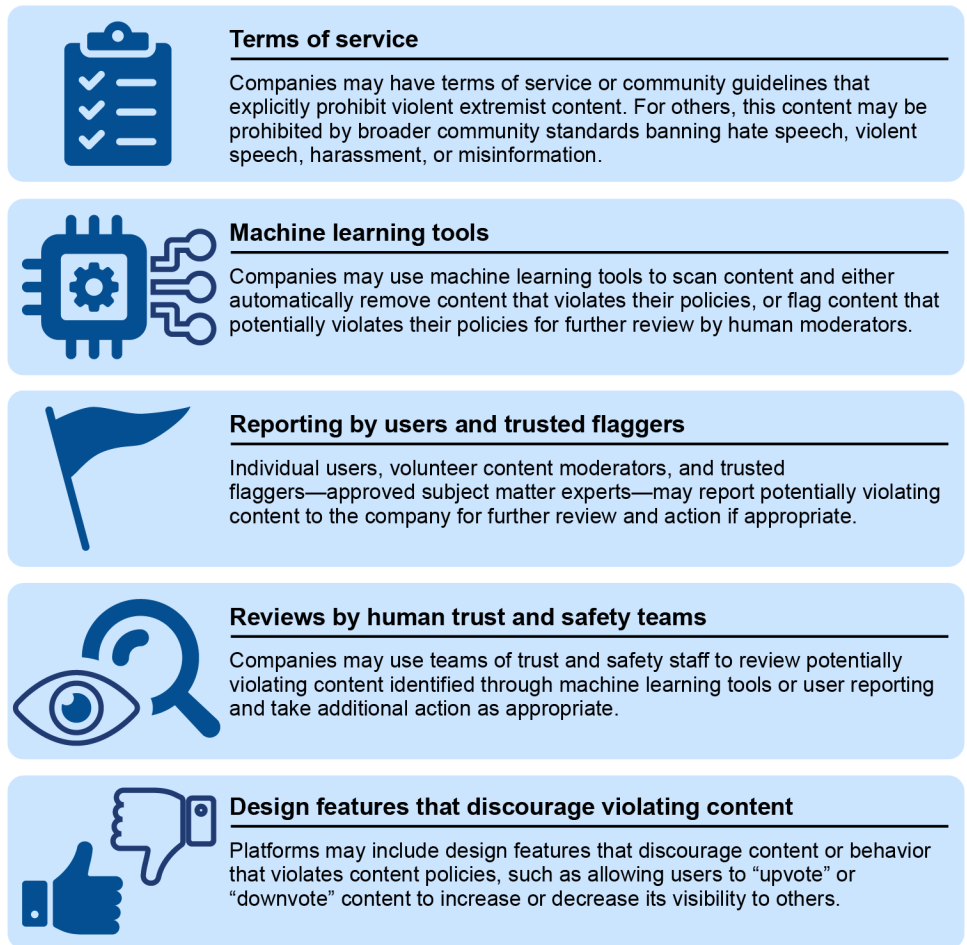
Selected Companies Reported Using Various Tools to Mitigate Content that Promotes Domestic Violent Extremism

Select Companies Reported Using Various Tools to Mitigate Content Promoting Domestic Violent Extremism

Social media and gaming companies we met with reported using various content moderation tools to identify and remove content promoting domestic violent extremism on their platforms. For example, all company officials we spoke with reported using terms of service provisions and various content moderation tools to identify and remove content promoting domestic violent extremism on their platforms. As private entities, companies can establish terms of service, such as community guidelines, that describe what kind of content they do not allow on their platform and may remove content that violates these terms, even if it is otherwise legal and protected under the First Amendment. Content moderation is a multi-layered process, and some company officials and experts told us that companies use the same tools for content promoting domestic violent extremism that they use for other content that violates their policies. See figure 4 for descriptions of these tools.

⁴¹Department of Homeland Security, Office of Intelligence and Analysis, *Domestic Violent Extremists Using Video Gaming-Adjacent Platforms for Nefarious Purposes* (Dec. 8, 2021).

Figure 4: Content Moderation Policies and Tools that Companies May Use



Source: GAO analysis of information from experts and social media and gaming companies; Icons-Studio/stock.adobe.com (illustrations), GAO (flag illustration). | GAO-24-106262

We selected 10 social media and gaming companies and reviewed the publicly available terms of service on their websites to determine whether these terms prohibited content promoting violent extremism on their platforms. The 10 companies we reviewed had the following terms of service:

- Five companies have publicly available terms of service explicitly prohibiting violent extremist content (Discord, Roblox, Twitch, X, and a social media company). Companies define this content in varying ways. For example, the game platform Roblox has an explicit, public-

facing policy prohibiting violent extremism on its platform. This is the only example of such a policy among major gaming companies, according to a December 2022 report by the Anti-Defamation League.⁴²

- Two companies (Reddit and a game publisher) have broader community guidelines prohibiting violent speech and content on their platforms, which company officials told us would cover content promoting domestic violent extremism. For example, the game publisher uses in-game codes of conduct that require players to show respect for others, among other things, which players must agree to adhere to before playing certain games.
- The other three companies in our sample have narrower policies stating that they prohibit illegal content on their platforms.

In addition, we interviewed officials from five companies to obtain additional information about the content moderation tools they report using. Company officials reported using the following tools:

- **Machine learning tools.** Officials from all five companies told us they use machine learning tools to scan content and either automatically remove content violating their policies, or flag potentially violating content for further review by human moderators. For example, officials from a social media platform told us they use an automated classification tool, which uses machine learning to scan posted content and classify it as violating the platform's policies. Officials from a game publisher said they work with companies specialized in online safety to deploy machine learning tools that classify, filter, and escalate disruptive interactions on the company's gaming platforms. Officials from two companies told us they participate in a collaborative effort by the industry-led Global Internet Forum to Counter Terrorism to assign unique digital signatures, known as "hashes," to distinct pieces of known violent extremist content in a database shared among participating companies.⁴³ The companies can then use a "hash-matching" tool to quickly identify and remove this content.

⁴²Anti-Defamation League, *Hate Is No Game: Hate and Harassment in Online Games 2022*.

⁴³The Global Internet Forum to Counter Terrorism is a non-governmental organization, founded in 2017, that seeks to foster collaboration between the technology industry, government, academia, and others to prevent terrorists and violent extremists from exploiting digital platforms.

Attacks on Law Enforcement Officers in California

In May 2020, an anti-government violent extremist attacked a federal courthouse in Oakland, California, killing one guard and injuring another. The following month, the same attacker killed a local law enforcement officer during an encounter in Ben Lomond, California.

Evidence established that the attacker adhered to the Boogaloo ideology, which emerged online and espouses an impending second Civil War driven by perceptions of government overreach. When law enforcement searched a vehicle registered to the attacker, they found a ballistic vest with a patch showing an igloo and Hawaiian-style print—symbols associated with Boogaloo. In the months leading up to the attack, the attacker's social media activity demonstrated a strong desire to carry out violent acts against federal law enforcement officers and other public servants. For example, the day before the courthouse shooting, the attacker posted a video of a mob attacking police cruisers, commenting, "This needs to be nationwide."

The attacker was sentenced to 41 years in prison.

Source: Department of Justice information. | GAO 24-106262

- **Reporting by users and trusted flaggers.** Officials from all five companies told us their platforms provide a way for users to report potentially violating content to the company for further review and action where appropriate. For example, the two gaming companies in our sample reported providing players with in-game features to report violating behavior that may not have been identified by machine learning. Two companies—Roblox and Discord—have a “trusted flagger” program, officials said, through which approved subject matter experts in extremism can use a streamlined channel to report potentially violating content. Further, Reddit officials told us that in addition to having a team of trust and safety employees who administer site-wide content policy, volunteer users (known as “moderators”) within individual communities (known as “subreddits”) create and enforce community-specific rules by manually reviewing content and applying automated filters.
- **Reviews by human trust and safety teams.** Officials from all five companies told us they have teams of staff who review potentially violating content identified through machine learning tools or user reporting. For example, Discord officials told us that they do not take any action against flagged content before it has been reviewed and confirmed as violating platform policies by a human reviewer. All five companies allow users to appeal moderation actions taken against them or their content and use human reviews as part of this process, officials told us. Two companies have staff who proactively monitor the behavior of bad actors on other platforms. Officials said this strategy may help them prevent violent extremist actors from misusing their platforms, and they can use their understanding of content on other platforms to better inform their own policies.
- **Design features that discourage violating content.** Officials from three of five companies we met with told us that their platforms include design features that may discourage content and behavior that violates platform policies. For example, Reddit officials told us that users on their site can “upvote” or “downvote” posts and comments, thereby increasing or decreasing their visibility to other users. This system helps suppress polarizing content and identify positive and negative behaviors, they said. Similarly, one online game uses features such as in-game incentives to discourage disruptive play and encourage positive behavior, according to officials at the game publisher. Some companies also use redirection tools, such as a tool that officials from one company described as redirecting users who search for certain violent extremist terminology to the website of a nonprofit organization that provides deradicalization resources.

In addition, officials from all five companies we spoke with told us they regularly review their content moderation policies and tools to ensure they are designed appropriately to capture violating content because of real-world events. For example, researchers have identified user-generated re-creations of mass shootings on the gaming platform Roblox, such as the 2019 shooting in Christchurch, New Zealand, and the 2022 shooting in Buffalo, New York.⁴⁴ Roblox officials told us their moderation team reviewed their content moderation tools and adjusted them to block these games and prevent content glorifying violent incidents from appearing on the platform.

In another example, in summer 2020, Reddit undertook a review of its content policies and, following conversations with staff, moderators, and outside organizations, rewrote one policy to explicitly state that communities and users “that incite violence or that promote hate based on identity or vulnerability will be banned.” All five companies we spoke with also told us they obtain and incorporate feedback as appropriate from subject matter experts, such as those in academia and special interest groups. For example, one company provides civil society organizations and researchers with a reporting channel and an opportunity to share feedback on content moderation policies.

Some company officials and experts also described initiatives to use social media and gaming platforms to prevent and counter domestic violent extremism. For more information, see appendix III.

Company Leadership, Financial Considerations, and Evasion Efforts Affect Company Efforts to Mitigate Content

Some company officials and experts we met with reported that efforts to mitigate content promoting domestic violent extremism are affected by company leadership, financial considerations, and efforts by users to evade content moderation.

Leadership Preferences and Financial Considerations

Most experts characterized leadership preferences and financial considerations at social media and gaming companies as factors affecting company content moderation efforts. Leadership preferences and company culture can result in limited content moderation efforts, according to most experts with whom we spoke. For example, some

⁴⁴In March 2019, a violent extremist committed a mass shooting at two mosques in Christchurch, New Zealand, and livestreamed the attacks online. In May 2022, a violent extremist committed a mass shooting at a grocery store in Buffalo, New York, after posting an online manifesto.

experts said some companies choose to have no or limited content moderation policies and practices on their platforms, or do not fully enforce the policies they have. As a result, enforcement by a few platforms is often not enough to prevent the spread of violent extremist content to other platforms. Some experts also noted that the existing legal framework is a limitation. For example, Section 230 of the Telecommunications Act of 1996 shields companies from being held liable for the user-generated content on their platforms.

As for-profit entities, social media and gaming companies make decisions at least in part based on financial considerations, most experts said. Companies that earn revenue through advertising have a financial incentive to keep user engagement and time on platform high, and may do this using recommendation algorithms. Most experts we spoke with said that recommendation algorithms can amplify polarizing and extreme content, thereby aiding in the spread of violent extremist content. However, one expert noted that not all platforms use recommendation algorithms. Another said that modifying the algorithms would not be enough to prevent the spread of this content, and that even without algorithms, violent extremist content would still exist and be easily findable online.

Further, the amount of resources companies use for content moderation can affect these efforts. Some experts noted that content moderation is expensive and does not generate revenue or directly serve the economic interests of for-profit companies. They also said that companies may expend just enough resources to avoid any reputational risk or scrutiny that may come with tolerating violent extremist content. Meanwhile, some larger companies may have large trust and safety teams dedicated to mitigating content that violates their policies, while smaller companies lack the same level of resources, experts told us. Two companies told us that they have limited resources to allocate to content moderation on their platforms. For example, one company said that video content moderation via the Global Internet Forum to Counter Terrorism “hash-matching” tool can be very expensive. In addition, in 2022 and 2023, some technology companies responded to financial pressures by reducing the size of their staff. Some experts told us that these reductions in staff, which included trust and safety staff, could negatively impact content moderation efforts.

Moderation Evasion Efforts

Most of the experts and companies we spoke with mentioned that the ever-changing and dynamic moderation evasion tactics pose a challenge to company efforts to mitigate content promoting violent extremism, which experts likened to a game of “whack-a-mole.” Violent extremists may use

coded language or edited versions of images or videos that human reviewers or machine learning content moderation efforts cannot quickly recognize as violent extremist content, experts and company officials told us. For example, the Boogaloo movement is known for using coded language and imagery—such as “Big Igloo” or an igloo emoji instead of “Boogaloo”—in their communication to evade content moderation, experts and company officials said. Another moderation evasion tactic is the conversion of violent extremist texts, such as mass shooter manifestos, into audiobooks to evade content moderation efforts that may be more constrained with audio content, according to an I&A report.⁴⁵

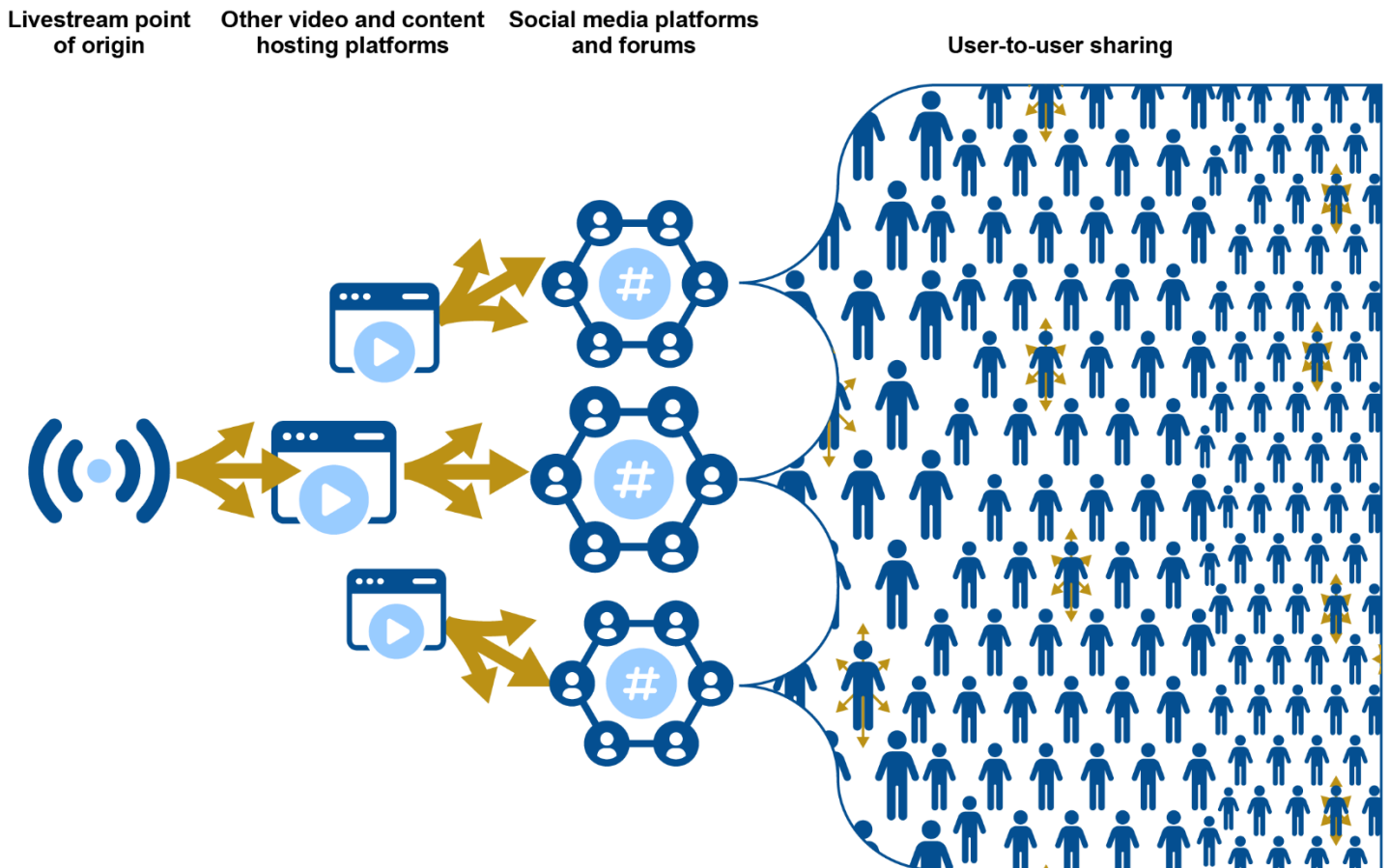
In addition, some experts told us that violent extremists use narratives and aesthetics in a more organic way that bypasses moderation efforts while still spreading their messaging. For example, some white supremacists appropriate ancient Greek, Roman, and Norse imagery to create an aesthetic that supports their narratives, two experts said. One of the experts noted that this type of imagery may not directly violate company content policies, but it helps draw others into this worldview.

Further, domestic violent extremists use a variety of platforms to circumvent moderation efforts. For example, officials from one company told us that violent extremist users may be aware of their terms of service and use the platform to maintain a less violence-oriented presence while simultaneously posting more openly on other platforms. Moderation actions by some platforms tend to push the affected users to other platforms that are more permissive toward their content, experts told us. This “deplatforming” has the benefit of exposing fewer users on mainstream platforms to violent extremist content, some experts said; however, deplatformed users can then move to different platforms and use their claims of censorship to attract followers and become more extreme, some experts told us.

According to DHS, FBI, and NCTC, online content can spread quickly within and across platforms even if the original post is quickly removed. For example, a livestream on a video streaming platform can be reposted across multiple platforms and accumulate a large number of views quickly (see figure 5 for a visual representation of broad dissemination).

⁴⁵Department of Homeland Security, Office of Intelligence and Analysis, *Racially or Ethnically Motivated Violent Extremist Messaging Likely Extends Reach Through Audio Narrations of Influential Literature* (Jan. 5, 2023).

Figure 5: Example of the Viral Nature of Domestic Violent Extremists' Use of Online Platforms



Source: GAO analysis of U.S. Department of Homeland Security, FBI, and National Counterterrorism Center information; Icons-Studio/stock.adobe.com. | GAO-24-106262

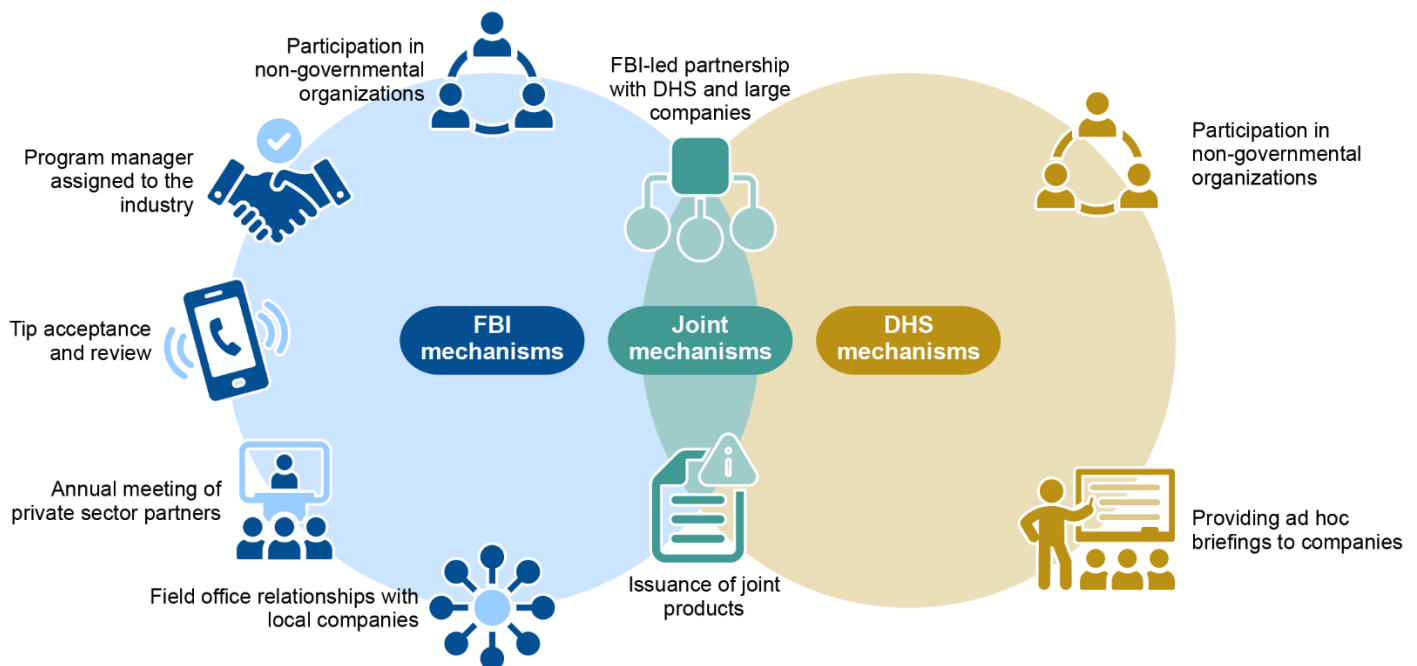
The FBI and DHS Have Not Developed Strategies for Information-Sharing with Social Media and Gaming Companies

The FBI and DHS both have several mechanisms for sharing information with, and receiving information from, social media and gaming companies about domestic violent extremism. However, neither agency has a cohesive strategy that encompasses these mechanisms, nor overarching goals for its information-sharing efforts with companies about online content that promotes domestic violent extremism.

The FBI and DHS Have Mechanisms for Sharing and Receiving Information from Social Media and Gaming Companies

The FBI and DHS have mechanisms for sharing information with, and receiving information from, social media and gaming companies about domestic violent extremism. Each agency has its own mechanisms for information-sharing with the companies, as well as joint information-sharing efforts (see figure 6).

Figure 6: Examples of FBI and DHS Mechanisms for Sharing Domestic Violent Extremism Information with Social Media and Gaming Companies



Source: GAO Analysis of Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) information; Icons-Studio/stock.adobe.com (icons). | GAO-24-106262

According to FBI officials, the agency has several mechanisms for sharing information with, or receiving information from, social media and gaming companies about domestic violent extremism. These mechanisms include:

- **Participation in non-governmental organizations.** The FBI participates in the Global Internet Forum to Counter Terrorism, as well as Tech Against Terrorism, which is an initiative the United Nations launched in 2016 to work with the global technology industry to combat terrorist use of the internet.
- **Program manager assigned to the industry.** The FBI has a dedicated program manager to oversee communications and

interactions with social media companies. According to FBI officials, the FBI and companies share threat information through the program manager. The FBI shares lessons learned from prior incidents, mobilization indicators of violent extremists, and information about reporting federal crimes and threats to life. Companies share concerns they have seen on their platforms, according to FBI officials.

- **Annual meeting of private sector partners.** The FBI holds an annual meeting with private sector partners, at which the FBI provides briefings and speakers on the current threat landscape. Officials said in 2023, the FBI worked to increase engagement with gaming and gaming-adjacent companies for the annual meeting and on outreach efforts with the program manager. Officials said that as the FBI works with more companies, it continues to learn how companies operate, the type of behavior and content companies see on their platforms, and the extent to which companies report information as tips.
- **Field office relationships with local companies.** Two companies told us they work closely with their local FBI field office and find that relationship to be valuable. For example, one company told us their FBI field office has a cyber squad that notifies them of trends in violent extremist content online, and another said their field office connects them with other federal agencies as needed.
- **Tip acceptance and review.** The National Threat Operations Center (NTOC) has been the FBI's centralized tip processing center since 2018. Members of the public, including officials from private sector entities, can submit tips to the FBI via NTOC. Four companies told us that when they identify a potential domestic violent extremist threat on their platform, they report the incident to the FBI for possible further investigation. NTOC processes the tips, conducting an initial evaluation and forwarding some tips to FBI field offices for further action, such as opening an investigation.

According to DHS officials, the agency has two mechanisms for sharing information with, or receiving information from, social media and gaming companies about domestic violent extremism:

- **Participation in non-governmental organizations.** DHS has participated in industry partnership organizations such as the Global Internet Forum to Counter Terrorism, Christchurch Call to Action, and

Extremism and Gaming Research Network.⁴⁶ These organizations bring together representatives from industry, government, and academia to foster collaboration and information sharing. According to officials, DHS's role in these organizations is to attend meetings and receive or share information about mobilization and radicalization online. For example, in April 2023, I&A attended Extremism and Gaming Research Network's monthly meeting and provided a briefing on an intelligence assessment product about domestic violent extremists' use of video gaming adjacent platforms. According to officials, I&A can also email intelligence products to representatives from these organizations.

- **Providing briefings to companies.** I&A provides briefings upon request to company trust and safety teams.⁴⁷ According to officials, I&A has provided about six briefings to social media and gaming companies since March 2021. At these meetings, officials said that I&A shared analysis about domestic violent extremism online, inquired whether companies would benefit from receiving additional

⁴⁶Christchurch Call to Action began in 2019 after a violent extremist committed a mass shooting at two mosques in Christchurch, New Zealand, and livestreamed the attacks online. Extremism and Gaming Research Network began in 2021 to build evidence and fill knowledge gaps to intervene in the exploitation of online gaming by terrorists and violent extremists.

⁴⁷In July 2023, I&A officials told us they continued to consult counsel prior to engaging in activities that could fall within the scope of a preliminary injunction that was issued pursuant to ongoing litigation in *Missouri v. Biden*, No. 3:22-CV-01213 (W.D.La, July 4, 2023). I&A officials stated they are refraining from such activities where necessary, while awaiting a final ruling. The preliminary injunction prohibited multiple defendants, comprised of several federal entities and named individuals sued in their official capacity, from coordinating and communicating with social media companies in a way that would infringe upon U.S. citizens' constitutional right to free speech, such as seeking the removal or suppression of content containing protected free speech. At the time we spoke with I&A officials, a stay of preliminary injunction was in effect pending appeal of the preliminary injunction in the Fifth Circuit, but I&A officials said they were continuing to exercise caution while awaiting a final ruling. On September 8, 2023, the Fifth Circuit affirmed in part and vacated in part the preliminary injunction. See *Missouri v. Biden*, No. 23-30445 (5th Cir., Sept. 8, 2023). Specifically, the court vacated the injunction in its entirety as it applied to DHS I&A, among other named defendants (revised opinion issued on October 3, 2023). An appeal of the Fifth Circuit's decision to the Supreme Court of the United States remains pending as to the remaining agencies, and, on October 16, 2023, the Supreme Court stayed the preliminary injunction, as modified by the 5th Circuit, until the Supreme Court issues its decision on the merits. DHS I&A is no longer limited by this case from interactions with social media companies but, as of January 2024, DHS remains a named defendant in the litigation, which is ongoing in the district court. As of January 2024, the FBI also remains a named defendant in the ongoing district court litigation. According to FBI officials, the FBI continues to proceed cautiously, adding an additional layer of review and approval by the FBI Office of the General Counsel with respect to certain communications with social media platforms.

information from federal agencies to support their independent content moderation efforts, and learned about technological and content moderation developments on the companies' platforms. Officials said social media and gaming companies may use these meetings to share information with I&A about online activities promoting domestic violent extremism, share information about activities that violate the companies' terms of service, and ask questions about I&A products and analyses.

According to officials, the FBI and DHS have two joint efforts for sharing information with, or receiving information from, social media and gaming companies about domestic violent extremism:

- **An FBI-led partnership with DHS and large companies.** The FBI provides briefings, awareness webinars, and other informational materials to Domestic Security Alliance Council member companies on a variety of threats to U.S. critical infrastructure, including domestic threats. One company told us this partnership is useful in providing frequent updates on domestic threats, such as intelligence briefings and email digests.
- **Issuance of joint products.** The FBI and DHS have issued joint informational products related to the online threat landscape. For example, NCTC, the FBI, and DHS issued a booklet on violent extremist mobilization indicators in 2021, as well as a spin-off booklet on the tech sector in 2022. The FBI co-briefed private sector entities alongside DHS and NCTC partners on this booklet. In addition, in 2017, several entities including DHS and the FBI developed the *Real-Time and Open Source Analysis Resource Guide* to help agencies and fusion centers understand the appropriate use of publicly available online information, focusing on social media.

The FBI and DHS Have Not Developed Goals or Strategies for Sharing Information About Domestic Violent Extremists with Social Media and Gaming Companies

The FBI and DHS have not developed goals or overarching strategies for sharing information with, and receiving information from, social media and gaming companies about domestic violent extremism. *Standards for Internal Control in the Federal Government* states that management should define objectives clearly, in terms that allow for the assessment of performance toward achieving objectives.⁴⁸ We have previously found that federal agencies should define goals, as a best practice to more

⁴⁸GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

effectively implement activities.⁴⁹ When an agency sets goals, it determines why it takes an action, while strategies determine how it takes an action. Developing goals and strategies can include internal or informal planning and coordination.

We found that the FBI and DHS have not developed goals or overarching strategies for information-sharing mechanisms with social media and gaming companies about domestic violent extremism. Specifically, neither agency has developed a strategy that articulates how it identifies and selects companies to engage with, or the goals and desired outcomes of its engagement with social media and gaming companies.

While officials reported that the FBI has goals associated with mitigation of international and domestic terrorism threats, officials noted that these goals are agnostic of the platforms used. FBI officials stated that they incorporate the use of social media and gaming platforms in investigations or addressing tips related to domestic violent extremist threats online, but there are no goals specifically associated with these topics. While the FBI generally seeks to build and maintain relationships with social media and gaming companies to better facilitate legal processes from field investigations and provide mechanisms for reporting federal crimes and threats to life to the FBI, it has not developed specific goals or strategies to determine how its efforts help to achieve those goals. According to FBI, the agency has had informal planning discussions internally as it works toward solidifying specific goals and strategies.

Keeping up with complex and dynamic threats from domestic violent extremists presents challenges for federal agencies as well as social media and gaming companies' content moderators. Developing goals and strategies could help the FBI and DHS determine how effectively each agency's information-sharing mechanisms align with and serve the agencies' overall missions, such as determining how effective the communications are with companies, and whether they are effectively selecting companies for information sharing. Setting program goals and overarching strategies specifically for sharing information with social media and gaming companies as it relates to domestic violent extremism is important to guide efforts and distinguish from other engagements, such as on foreign influence or foreign terrorism. Other engagements

⁴⁹GAO, *Evidence-Based Policymaking: Practices to Help Manage and Assess the Results of Federal Efforts*, [GAO-23-105460](#) (Washington, D.C.: July 12, 2023).

may have different goals and implementation may follow different guidelines.

The FBI and DHS both have ongoing efforts to engage with companies about domestic violent extremist threats, and companies we spoke with identified a variety of different methods, frequencies, and subjects when describing their communications with the FBI and DHS. The FBI has at least one Private Sector Coordinator in each field office to engage with companies in their area of responsibility on a variety of threats and topics. Private Sector Coordinators are able to connect companies concerned about domestic violent extremist threats with FBI field office investigative squads, for example. The FBI developed a one-page document describing the role of the Private Sector Coordinator at each field office, a way to contact them, and information about other FBI information-sharing mechanisms. DHS has also developed briefings to provide to companies upon request. However, distribution of these materials is ad hoc and not reflected in a cohesive strategy. Organizing efforts and mechanisms under a strategy to achieve identified goals and outcomes can help the agencies implement them more effectively and leverage resources. For example, I&A officials believed that they were sharing intelligence assessments with social media and gaming companies through the Homeland Security Information Network portal. However, the portal's program management office told us no social media and gaming companies have access to the portal. Therefore, I&A officials did not have complete information about the audience of their intelligence assessments, or the extent to which DHS shares information with social media and gaming companies.

DHS officials reported that DHS has not set program goals for its information-sharing mechanisms between agencies and companies about domestic violent extremism because it is in the process of developing goals for its partner engagement activities more broadly. I&A officials noted its private sector information-sharing efforts in this area are evolving, as it established its Domestic Terrorism Branch in March 2021, and a directorate of partnerships in October 2022. According to officials, I&A is in the process of developing goals that more fully describe its partnership engagement activities, but it expects information sharing with social media and gaming companies to be a narrow piece of those broader goals.

According to officials, the FBI has a broad goal to build and maintain relationships with social media and gaming companies, to better facilitate investigations, and provide mechanisms for companies to report federal

crimes and threats to life. However, we did not find evidence of more specific goals than enhancing relationships with companies, or strategies to determine how the FBI's efforts help to achieve those goals. The FBI also has broad goals related to engagement with the private sector.

The FBI has not set specific goals because much of its partner engagement in this area is a relatively new effort, and because the FBI follows broad guidance and goals related to private sector engagement and counterterrorism. Developing goals and strategies can include internal or informal planning and coordination with each agency and can supplement or provide iterative updates to formal agency efforts. Setting goals and identifying a strategy for sharing information on domestic violent extremism threats can help the FBI and DHS align their resources and ensure their efforts are meeting their needs.

Conclusions

The FBI and DHS have identified domestic violent extremists as one of the most significant terrorism threats to the U.S. today and reported that many of these extremists are radicalized online or are active online. These agencies, as well as the social media and gaming companies that operate online platforms, have a critical role to play in protecting against domestic violent extremism. The FBI and DHS have been taking steps to engage with social media and gaming companies to share information on threats related to domestic violent extremism. However, the FBI and DHS have not developed goals and strategies related to these information-sharing efforts. By establishing program goals and strategies, the FBI and DHS can help ensure that the mechanisms align with and serve the agencies' overall missions.

Recommendations for Executive Action

We are making the following two recommendations, one each to the FBI and I&A:

The Director of the FBI should develop a strategy and goals for sharing information related to domestic violent extremism with social media and gaming companies. (Recommendation 1)

The Under Secretary for Intelligence and Analysis should develop a strategy and goals for sharing information related to domestic violent extremism with social media and gaming companies. (Recommendation 2)

Agency Comments

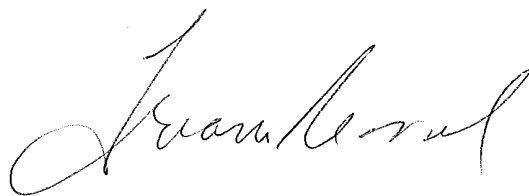
We provided a draft of this report to DHS, DOJ, and the Office of the Director of National Intelligence (ODNI) for review and comment. DHS and DOJ concurred with our recommendations. DHS provided a comment

letter which is reproduced in appendix IV. DHS, DOJ, and ODNI also provided technical comments, which we incorporated, as appropriate.

In its letter, DHS indicated that I&A plans to develop an information sharing strategy that will describe, among other things, how I&A will establish goals and desired outcomes for efforts designed to improve communications with social media and gaming companies. DHS expects to complete the strategy by June 2024. If implemented, we expect the strategy to provide guidance to I&A's information sharing efforts with social media and gaming companies.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the appropriate congressional committees, the Attorney General, the Secretary of Homeland Security, the Director of National Intelligence, and other interested parties. In addition, the report will be available at no charge on the GAO website at <https://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-8777 or McNeilT@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.



Triana McNeil
Director, Homeland Security and Justice

Appendix I: Experts Who Participated in GAO's Interviews and Relevant Affiliations

Table 1: Experts Who Participated in GAO's Interviews and Relevant Affiliations

Expert	Affiliations
John Cohen	Center for Internet Security
Meghan Conroy	Atlantic Council Digital Forensic Research Lab and Accelerationism Research Consortium (ARC)
Jack Donohue	Network Contagion Research Institute (NCRI)
Alex Goldenberg	NCRI
Jenna Hopkins	Anti-Defamation League (ADL)
Brian Hughes	American University Polarization and Extremism Research and Innovation Lab
Lauren Krapf	ADL
Matt Kriner	Middlebury College Center on Terrorism, Extremism, and Counterterrorism, and ARC
Galen Lamphere-Englund	Extremism and Gaming Research Network (EGRN)
Brian Levin	California State University San Bernardino Center for the Study of Hate and Extremism
Jon Lewis	George Washington University Program on Extremism
Pete Simi	Chapman University
Megan Squire	Southern Poverty Law Center
Talya Steinberg	ADL
Jessica White	Royal United Services Institute and EGRN
Heather Williams	RAND Corporation

Source: GAO. | GAO-24-106262

Appendix II: FBI and DHS Views Related to their Efforts to Address Online Content Promoting Domestic Violent Extremism

Agency officials we spoke with shared views related to their efforts to address online content promoting domestic violent extremism. For example:

- **Keeping up with a rapidly evolving issue.** Violent extremists continuously change coded language and tactics, according to experts. Lines are blurred between groups that share followers, increasingly mobilize together, and do not have formal membership. Violent extremists migrate to more permissive platforms or change their terminology. For example, according to a National Fusion Center Association official, social media users plotting the January 6, 2021 attack on the U.S. Capitol used code words for weapons, so they could covertly discuss plans to bring weapons to the Capitol.

Agencies take steps to continually update their understanding of online content that promotes domestic violent extremism. For example, the FBI creates Domestic Terrorism Reference Guides, which are designed to provide a high-level overview of a particular threat topic. In addition, the intelligence assessments that I&A creates and shares with partners can include topics related to the online domestic violent extremist landscape. I&A updates intelligence assessments when officials believe the threat has evolved significantly since the last assessment on that topic.

- **Collecting information on gaming platforms.** According to I&A officials, personnel collect information from social media platforms, but not gaming platforms. Officials said most gamers prefer private servers where the players they interact with are there by invitation, so I&A personnel would not have access to most game sessions. They also said most gamers communicate via microphone. I&A collects text and images, but not audio. Lastly, officials said personnel are required to collect publicly available information in ways that do not involve interaction with other users, and that their presence is not observable by other users, which would not be possible in most games.

Appendix III: Efforts to Prevent and Counter Violent Extremism on Online Platforms

Experts we spoke with described several types of initiatives that researchers and companies have explored to use social media and gaming platforms to prevent and counter violent extremism. Overall, experts said these initiatives are still new and more research is needed on their effectiveness and scalability.

- **“Inoculation” and digital literacy.** Some experts mentioned emerging research on and application of tools that teach users about manipulative online content, thereby “inoculating” them against it. For example, American University’s Polarization and Extremism Research and Innovation Lab worked with Google to develop a 30-second video to air on YouTube before content, which can help users recognize the signs of manipulative video content. In addition, one expert suggested that the federal government can assist states in developing educational programs to teach parents how their children could be radicalized online, framing the issue as one of child safety.
- **Games to prevent radicalization.** One expert told us about games designed with radicalization prevention in mind, such as games that teach people how to identify misinformation. For example, Middlebury College’s Center on Terrorism, Extremism, and Counterterrorism received a grant from DHS to design a simulation game and curriculum to build resilience among adolescent internet users who may be exposed to violent extremism online. However, one expert said it is difficult to incorporate counter-radicalization concepts into larger, commercially available games, such as first-person shooters. As a result, it is not clear how successful or scalable this strategy is, the expert said.
- **Redirection.** Some experts and companies told us about redirection tools, which direct a user who searches for pre-identified keywords associated with violent extremism toward other content. For example, one expert told us about the company Moonshot, which works with online platforms to place ads challenging violent extremist narratives in the search results and social media feeds of certain users, according to the company’s website.
- **Positive messaging.** Some experts mentioned public service campaigns that encourage online influencers to weave positive messaging into their content, such as YouTube’s Creators for Change program. Two experts said that gaming spaces have strong community-building potential, and incorporating positive social narratives into these communities could help prevent radicalization. For example, some major sports leagues have launched “no hate”

**Appendix III: Efforts to Prevent and Counter
Violent Extremism on Online Platforms**

campaigns, a tool that could be applied to the digital space as well, one expert said.

Appendix IV: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

December 21, 2023

Triana McNeil
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to Draft Report GAO-24-106262, "Countering Violent Extremism: FBI and DHS Need Strategies and Goals for Sharing Threat Information with Social Media and Gaming Companies"

Dear Ms. McNeil:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

DHS leadership is pleased to note GAO's positive recognition of DHS's mechanisms for sharing and receiving threat-related information with social media and gaming companies. GAO also recognized that DHS, through its Office of Intelligence and Analysis (I&A), has made strides in its ongoing efforts to engage with companies about domestic violent extremist threats, including by establishing its Domestic Terrorism Branch in 2021 and its Office of Partnerships in 2022. As GAO notes, I&A is already developing goals that more fully describe its partnership engagement activities, which will include information sharing with social media and gaming companies as one aspect of those goals.

DHS remains committed to identifying, assessing, and sharing intelligence and information, as appropriate, with Federal, State, local, Tribal, territorial, and private sector partners with homeland security responsibilities to assist in the deterrence, prevention, preemption of, and response to terrorist attacks against the United States. This includes terrorism conducted by domestic violent extremists, one of the most significant terrorist threats to the United States today.


**Appendix IV: Comments from the Department
of Homeland Security**

The draft report contained two recommendations, including one for DHS with which the Department concurs. Enclosed find our detailed response to the recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H
CRUMPACKER

 Digitally signed by JIM H
CRUMPACKER
Date: 2023.12.21 08:30:43 -05'00'

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Enclosure

**Enclosure: Management Response to Recommendations
Contained in GAO-24-106262**

GAO recommended that the Under Secretary for Intelligence and Analysis:

Recommendation 2: Develop a strategy and goals for sharing information related to domestic violent extremism with social media and gaming companies.

Response: Concur. The Under Secretary for Intelligence and Analysis, acting through the I&A's Strategy, Plans, and Policy Division in coordination with (1) its Analytic Advancement Division; (2) Counterterrorism Center's Domestic Terrorism Branch; (3) Engagement, Liaison, and Outreach Division's Private Sector Engagement Branch; and (4) the Cybersecurity and Infrastructure Security Agency, will develop an information sharing strategy describing how I&A will:

- Share information,
- Facilitate access to this information through appropriate information sharing platforms,
- Promote access to and use of such platforms for relevant companies, and
- Establish goals and desired outcomes for the effort that are designed to improve I&A's communications with social media and gaming companies.

Estimated Completion Date: June 28, 2024.

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Triana McNeil at (202) 512-8777, McNeilT@gao.gov

Staff Acknowledgements

In addition to the contact named above, Kevin Heinz (Assistant Director), Emily Flores (Analyst-in-Charge), Simon Chan, Marissa Esthimer, Eric Hauswirth, Amanda Miller, Kevin Reeves, and Mary Turgeon made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548

