United States Government Accountability Office

Report to Congressional Requesters

January 2024

ONLINE EXTREMISM

More Complete Information Needed about Hate Crimes that Occur on the Internet

Accessible Version

GAO Highlights

ONLINE EXTREMISM

More Complete Information Needed about Hate Crimes that Occur on the Internet

Why GAO Did This Study

A hate crime occurs nearly every hour in the U.S., based on data reported to the FBI. Investigations of recent hate crimes have suggested that exposure to hate speech on the internet may have contributed to the attackers' biases against their victims. In 2021, the FBI placed hate crimes at the same national threat priority level as preventing domestic violent extremism.

GAO was asked to review information on hate crimes and hate speech on the internet. This report examines (1) the extent to which DOJ collects data on hate crimes that occur on the internet, (2) what company data indicate about steps selected companies have taken to remove hate speech and violent extremist speech from their internet platforms, and (3) what is known about users' experience with, or expression of, hate speech on the internet, and its relationship to hate crimes and domestic violent extremism.

GAO analyzed U.S. hate crime data and interviewed DOJ officials. GAO analyzed data and interviewed officials from six selected companies operating internet platforms with publicly available policies prohibiting hate and violent extremist speech. GAO assessed peer reviewed and nonprofit studies that described hate speech on the internet, hate crimes, and domestic violent extremist incidents.

What GAO Recommends

GAO recommends that BJS explore options to measure bias-related criminal victimization that occurs on the internet through the National Crime Victimization Survey or in a supplemental survey, as appropriate. BJS agreed with this recommendation.

What GAO Found

The Department of Justice (DOJ) collects data about hate crimes (i.e., crimes that manifest evidence of prejudice based on race, ethnicity, gender, gender identity, religion, disability, or sexual orientation) using two statistical programs:

- The Federal Bureau of Investigation's (FBI) Uniform Crime Reporting Program collects hate crime data, including hate crimes that occur on the internet, from law enforcement agencies.

- The Bureau of Justice Statistics (BJS) uses a national annual household survey—the National Crime Victimization Survey—to produce estimates of the prevalence of hate crimes reported and not reported to law enforcement. BJS's survey does not collect data on hate crimes that occur on the internet.

The 2022 Better Cybercrime Metrics Act requires BJS to include questions relating to cybercrime victimization in its survey. BJS funded a study that examined one method to measure bias-motivated victimization on the internet. However, the study did not explore other methods, such as an approach similar to how the survey measures in-person hate crimes. Exploring other options to measure bias-related criminal victimization on the internet in the National Crime Victimization Survey or a supplemental survey would complement FBI's data and help DOJ identify and provide assistance to communities affected by hate.

GAO found that all six selected companies took some steps to remove content that their policies defined as hate speech or promoting violent extremism against people based on actual or perceived characteristics, such as race or religion. The companies' data show the amount of hateful content removed varied across platforms they operated from 2018 through 2022. This is due in part to the variation of the company definitions of hateful content and their related policies.

Hate Speech Occurs on the Internet

Source: David Carillet/stock.adobe.com. | GAO-24-105553

Research indicates that up to a third of internet users reported they experienced hate speech on the internet, and users who post hateful or extremist speech on the internet may do so because the internet helps spread hateful ideologies. In addition, research and government reports indicate an association between hate speech on the internet and hate crimes. For example, one peer-reviewed research study found an association between uncivil comments on the internet and hate crimes against Asians in selected U.S. cities. Also, the Department of Homeland Security and the FBI reported that the internet created opportunities for individuals to self-radicalize and conduct lone offender attacks without the support of a larger violent extremist organization.

Contents

Table

Figures

Abbreviations
BJS   Bureau of Justice Statistics
DHS   Department of Homeland Security
DOJ   Department of Justice
FBI   Federal Bureau of Investigation
NIBRS   National Incident-Based Reporting System
UCR   Uniform Crime Reporting

January 12, 2024

The Honorable Jamie Raskin
Ranking Member
Committee on Oversight and Accountability
House of Representatives

The Honorable Richard Blumenthal
United States Senate

A hate crime occurs nearly every hour on average in the U.S., based on data reported by law enforcement agencies to the U.S. Department of Justice's (DOJ) Federal Bureau of Investigation (FBI).[1] According to DOJ, hate crimes and hate incidents pose a unique and distinct harm in our society. DOJ's National Institute of Justice reported in 2021 that hate crimes have a broader effect than most other kinds of crimes because the victims are not only the crime's immediate target but also others like them.[2] In 2021, the FBI elevated hate crimes to its highest-level national threat priority to address the rise of such crimes. FBI's designation placed hate crimes at the same priority level as preventing ideologically

---

[1]See: Rashawn Ray, *Preventing racial hate crimes means tackling white supremacist ideology*, (The Brookings Institution, May 17, 2022). In 2021, law enforcement agencies reported to the FBI that 10,957 hate crimes occurred in the U.S. In the U.S., there is no singular statutory definition of a hate crime. The Hate Crime Statistics Act, as amended, requires the Attorney General to collect data about crimes that manifest evidence of prejudice based on race, religion, disability, sexual orientation, ethnicity, gender, and/or gender identity. 34 U.S.C. § 41305. Federal and state criminal statutes may define a hate crime differently and may include additional protected categories. For example, one federal hate crime statute identifies familial status as an additional protected category. 42 U.S.C. § 3631.

[2]National Institute of Justice, *Overview of Hate Crime*, (Washington D.C.: Sept. 13, 2021).

motivated attacks carried out by the most significant domestic violent extremists.[3]

In recent years, investigations of hate crimes resulting in numerous fatalities revealed that perpetrators have at times used the internet to post hateful content prior to, or during, their attacks. For example, investigations of mass shootings at Emanuel African Methodist Episcopal Church in Charleston, South Carolina in 2015; a Walmart in El Paso, Texas in 2019; and a nightclub in Colorado Springs, Colorado in 2022, illustrated how exposure to hate speech on the internet may also have contributed to the attackers' bias against people based on their race, national origin, and sexual orientation.[4] Additionally, these attacks showed how the internet has offered perpetrators a vehicle for disseminating hateful material, such as posting manifestos containing disparaging and racist rhetoric prior to attacks. The perpetrators of these three attacks were convicted of or pled guilty to federal or state hate crimes.

Various nongovernmental entities have raised questions about whether increases in hate speech on the internet could lead to increases in hate crimes. Some internet-based platforms—such as social media platforms—have adopted policies that prohibit users from sharing content containing hate speech or violent extremist speech. However, a number of nongovernmental organizations have raised questions about whether hate speech and violent extremist speech continue to proliferate on the internet.

---

[3]According to the FBI and the Department of Homeland Security (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 other foreign power, who seeks to further political or social goals wholly or in part through unlawful acts of force or violence dangerous to human life (according to DHS officials, DHS also includes unlawful acts of force or violence potentially destructive of critical infrastructure). However according to the FBI and DHS's Strategic Intelligence Assessment, the mere advocacy of political or social positions, political activism, use of hateful rhetoric, or generalized philosophical embrace of violent tactics does not constitute extremism and may be constitutionally protected. FBI and DHS, *Strategic Intelligence Assessment and Data on Domestic Terrorism* (Washington, D.C.: June 2023). In FBI and DHS documentation, the terms domestic terrorist and domestic violent extremist are used interchangeably.

[4]For the purposes of this report, hate speech is defined as derogatory speech against individuals or groups based on their actual or perceived characteristics such as race, color, religion, ethnicity, national origin, gender, gender identity, disability, or sexual orientation.

You asked us to analyze available data about hate crimes and hate speech that occur on the internet, and the relationship between hate speech on the internet and hate crimes and domestic violent extremism. This report examines: (1) the extent to which DOJ collects data on hate crimes that occur on the internet;[5] (2) what company data indicate about steps selected companies have taken to remove hate speech and violent extremist speech from their internet platforms; and (3) what is known about users' experience with, or expression of, hate speech on the internet, and the relationship between hate speech on the internet and hate crimes and domestic violent extremism.

To address our first objective, we analyzed data from the FBI's Uniform Crime Reporting (UCR) Program on hate crimes that occurred on the internet between January 2016 and December 2021, the most recent data available during the time of this review.[6] This enabled us to describe the total number of reported hate crimes that occurred on the internet, as well as the types of offenses and bias motivations associated with the crimes. To determine the reliability of these data, we reviewed FBI documentation about policies and procedures for law enforcement agencies to report hate crimes to the FBI's UCR Program, such as FBI's *Hate Crime Data Collection Guidelines and Training Manual*.[7] We also interviewed DOJ officials from FBI's Criminal Justice Information Services Division about the standards, policies, and procedures that the FBI's UCR Program uses to collect data on hate crimes that occur on the internet

---

[5]For the purposes of this report and based on FBI documentation, hate crimes on the internet refer to hate crimes that occur over a virtual or internet-based network of two or more computers in separate locations which communicate either through wireless or wire connections.

[6]Since the passage of the Hate Crime Statistics Act in 1990, the FBI has used its UCR Program to collect crime data from federal, state, local, tribal, and university law enforcement agencies. See generally 34 U.S.C. § 41305. The UCR Program generates statistics for use in law enforcement. It also provides information for students of criminal justice, researchers, the media, and the public. The UCR Program includes data from more than 18,000 city, university and college, county, state, tribal, and federal law enforcement agencies. In 2016, the UCR Program began collecting information on hate crimes that occur on the internet. We analyzed annual data on hate crime incidents that the FBI provided to us in July 2023 and reported incidents that met quality review standards provided by FBI officials. FBI officials told us that the full calendar year data for 2022 would not be available until fall 2023.

[7]FBI, Criminal Justice Information Services Division, *Hate Crime Data Collection Guidelines and Training Manual*, Version 3.0 (Washington, D.C.: March 1, 2022).

from federal, state, local, tribal, and university law enforcement agencies.[8] Furthermore, we conducted electronic data testing to identify outliers and ensure the completeness of the data. We determined that the FBI's UCR data were reliable for the purposes of describing the extent and characteristics of DOJ's collection of data on hate crimes on the internet.

In addition, we interviewed DOJ officials from FBI's Criminal Justice Information Services Division and DOJ's Office of Justice Programs about support or technical assistance DOJ provides to law enforcement agencies to improve the collection of FBI's UCR data on hate crimes. We also interviewed six selected law enforcement agencies and one state UCR Program about how they collect and report data on hate crimes that occur on the internet to FBI's UCR Program. We selected agencies to interview based on a variety of factors that included variation in geographic dispersion, population size of the agency's jurisdiction, agency type (such as city, county, university, state, or federal), and the extent to which they reported hate crimes on the internet between 2016 and 2020.[9]

We also reviewed reports authored by or commissioned by DOJ's Bureau of Justice Statistics (BJS) regarding the National Crime Victimization Survey's collection of bias-motivated victimization data, such as *Enhancing the Measurement of Hate Crime in the National Crime Victimization Survey: Developing and Testing Improvements to the Survey Questions*.[10] Additionally, we interviewed BJS officials regarding procedures for the collection of such data and any steps the bureau was taking to revise the survey to collect data on criminal victimization committed on the internet. We reviewed BJS' plans for revising the survey and compared them to requirements outlined in the Better Cybercrime Metrics Act, *Standards for Internal Control in the Federal Government*

---

[8]For the purposes of this report, the term "local law enforcement agencies" refers to local, tribal, and university law enforcement agencies collectively.

[9]At the time of selection, 2020 was the last complete year of UCR data on hate crimes available from the FBI. The agencies we interviewed were FBI's Washington, D.C. Field Office; Lexington (Kentucky) Police Department; New Jersey State Police Department; Skagit County (Washington) Sheriff's Office; University of Michigan Police Department; Vermont State Police Department; and Worcester (Massachusetts) Police Department.

[10]Sarah Cook, Chris Krebs, Yuli Patrick Hsieh, Lynn Langton, and Jerry Timbrook, *Enhancing the Measurement of Hate Crime in the National Crime Victimization Survey: Developing and Testing Improvements to the Survey Questions*, NCJ 301033 (Research Triangle Park, North Carolina: RTI International, 2021).

related to using quality information, and the goals outlined in DOJ's Fiscal Years 2022-2026 Strategic Plan.[11]

To address our second objective, we analyzed data and interviewed officials from six selected companies that operate internet-based platforms regarding their enforcement of policies on hate speech and violent extremism.[12] To identify which companies to include in our review, we examined 25 studies published between June 2016 and June 2022 from nongovernmental organizations about hate speech on the internet and its relationship to hate crimes and domestic violent extremism.[13] We also reviewed 94 news articles published between June 2019 and June 2022 describing hate crimes or domestic violent extremist incidents that recently occurred. We counted how often studies and news articles cited companies' internet-based platforms as where hate speech or violent extremist speech occurred. We organized the companies by the number of citations from most to least, and by type of service the companies' platforms provided, such as crowdfunding, livestreaming, or social media.

We reviewed whether the companies' publicly available policies explicitly defined and prohibited platform users from using hate speech or violent extremist speech. We then interviewed officials from the most cited companies that had publicly available hate speech or violent extremist speech policies, regarding how they enforce these policies and regarding what data the companies track and publish about their enforcement of these policies. Finally, we analyzed publicly available data, and data that six companies provided to us, to describe the amount of content and number of users that violated the hate speech or violent extremist speech policies from January 2018 through December 2022, for seven platforms operated by six companies.[14] We analyzed enforcement data from

---

[11]Pub. L. No. 117-116, 136 Stat. 1180 (2022); GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014): U.S. Department of Justice, *Fiscal Years 2022-2026 Strategic Plan,* (Washington, D.C.: 2022).

[12]Companies may use community guidelines, policies, and terms of service to define what users are prohibited from doing—such as defining types of prohibited text, images, and audio (i.e., violative content)—on the companies' platforms. For the purposes of this report, we will refer to these collectively as policies.

[13]We selected this time frame to capture information to match the time frame used in the first objective.

[14]Three of the companies operated four social media platforms. The other three companies operated a livestreaming and media-hosting platform, a communication and messaging platform, and a crowdfunding and financial transactions platform, respectively.

companies in six-month time periods—January through June and July through December—when complete data were available.

To address our third objective, we conducted a review of literature published from January 2016 through October 2022 to describe available research about hate speech on the internet and its relationship to hate crimes and domestic violent extremism in the U.S.[15] Sources included publications by nonprofits and think tanks, in addition to various databases and platforms that host scholarly and peer-reviewed publications. For example, we used ProQuest, EconLit, Homeland Security Digital Library, Scopus, and WorldCat, to identify relevant studies. We excluded conference proceedings, trade journal articles, law review articles, news articles, and summaries of congressional hearings and updates on bills as they move through congressional committees from the literature review. We selected studies to review that focused on U.S. users or internet platforms operating in the U.S., where the type of online hate speech or extremist ideology examined was motivated by bias towards a person's perceived or actual race, color, religion, ethnicity, national origin, sexual orientation, gender, gender identity, or disability. We reviewed 53 studies, which contained information on one or more of the following themes: (1) the demographic characteristics of users who post hate speech, the effect of this behavior on other users, or the format of hate speech posted online, (2) how internet users are motivated to post or participate in hate speech online or join groups or online spaces that facilitate this type of rhetoric, (3) specific time periods or catalyzing events relevant to the online hate speech discussed in the study, and (4) the linkage, if any, between online hate speech and off-line real world attacks.[16]

Additionally, we reviewed DOJ, FBI, and Department of Homeland Security (DHS) reports about hate crimes, including reports about criminal incidents we characterize as involving bias-motivated domestic violent extremism.[17] In addition, we interviewed DOJ, FBI, and DHS officials to describe when these federal agencies have found evidence of a

---

[15]We selected this time frame to capture information to match the time frame used in the first objective.

[16]We also recorded any policy recommendations and discussions of the limitations of the research relevant to one or more of the four themes.

[17]In this report, we refer to bias-motivated domestic violent extremism as violent extremism ideologies in the territorial U.S. that are motivated by bias against protected characteristics identified in federal hate crime statutes.

perpetrator's hate speech on the internet as part of the agencies' investigations of hate crimes or violent extremist incidents. We also reviewed DOJ press releases regarding federal prosecutions of hate crimes for 2016 through 2022, to describe instances when DOJ indicated a perpetrator's hate speech on the internet was used as evidence in prosecutions. Additionally, DHS provided us with information on domestic terrorism incidents DHS collected and tracked from 2016 through 2022.[18] We analyzed DHS's data to identify when an incident included information that we assessed as hate speech posted to the internet by a perpetrator prior to carrying out a domestic terrorism incident. For a more detailed discussion of our scope and methodology, see appendix I.

We conducted this performance audit from November 2021 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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Hate Speech, Hate Crimes, Domestic Terrorism, and Bias-Motivated Domestic Violent Extremism

For the purposes of this report, hate speech is defined as derogatory speech against individuals or groups based on their actual or perceived characteristics such as race, color, religion, ethnicity, national origin, gender, gender identity, disability, or sexual orientation. Hate speech alone is not a crime and may be subject to constitutional protections.[19] However, there are circumstances in which hate speech may lose constitutional protection and represent a crime itself if the speech, for

---

[18]We selected this time frame to capture information to match the time frame used in the first objective.

[19]The First Amendment states that Congress shall make no law abridging the freedom of speech. U.S. CONST. amend. I. To this point, the First Amendment protects a broad range of speech and expression, even if such speech may be considered unsavory or offensive. Therefore, the First Amendment generally protects a speaker's right to make derogatory statements on the internet against individuals or groups sharing protected characteristics (hate speech on the internet).

example, breaches the threshold of a "true threat."[20] In such instances, hate speech expressed on the internet may be prosecuted as a crime if the hate speech communicated serious intent to commit violence against others.

Statutory hate crimes criminalize specific conduct that is motivated by bias toward the victim's actual or perceived characteristics as defined in statute. Hate speech can be used in the prosecution of a hate crime as evidence to prove the offender acted "because of" the victim's protected characteristics.[21] According to DOJ, there are four federal statutes under which DOJ can prosecute hate crimes. These statutes collectively protect against certain crimes based on bias against a victim's race, color, religion, national origin, sexual orientation, gender, gender identity, disability, or familial status.[22] Federal and state criminal statutes may define hate crimes differently and may include different protected

---

[20]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 and may constitute a criminal act. More specifically, such speech may be considered a hate crime if the necessary additional elements of the crime (e.g., bias motivation) are met. In some cases, federal prosecutors have also presented evidence of a perpetrator's off-line activity to demonstrate the seriousness of the threat, thus showing that the threat made on the internet was credible and "true." See *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*, No. 22-138 (U.S. June 27, 2023) (holding that in an online threatening communications case, the State must prove that the defendant had some subjective understanding of their statements' threatening nature).

[21]In other words, the prosecution may use hate speech as evidence of the offender's bias motivated intent, which is necessary to meet the elements of the offense.

[22]According to DOJ, the four hate crime statutes are: (1) The Matthew Shepard and James Byrd, Jr. Hate Crimes Prevention Act, 2009 (Pub. L. No. 111-84, Div. E, § 4707, 123 Stat. 2190, 2838 (2009) (codified at 18 U.S.C. § 249)); (2) Damage to Religious Property, Church Arson Prevention (18 U.S.C. § 247); (3) Violent Interference with Federally Protected Rights (18 U.S.C. § 245); and (4) Criminal Interference with the Right to Fair Housing (42 U.S.C. § 3631). Further, according to DOJ, additional statutes may be used to prosecute crimes that may include bias motivation such as 18 U.S.C. §§ 875, 876, which allow for the prosecution of an individual for sending threatening communications through the mail or commerce. However, these additional statutes do not require DOJ to prove a bias motivation and are therefore not characterized as hate crime statutes.

categories.[23] According to DOJ, 48 states and the District of Columbia have hate crime laws that cover some or all protected categories identified in federal hate crime statutes.[24] DOJ is responsible for enforcing federal hate crime laws, while state hate crime laws are enforced by state and local law enforcement agencies.

According to the FBI and DHS' *Strategic Intelligence Assessment and Data on Domestic Terrorism* report issued in June 2023, the FBI defines a domestic terrorism incident as a criminal act, including threats or acts of violence to specific victims, made in furtherance of a domestic political and/or social goal, which has occurred and can be confirmed.[25] 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 other foreign power, who seeks to further political or social goals wholly or in part through unlawful acts of force or violence dangerous to human life.[26] In FBI and DHS documentation, the terms domestic terrorist and domestic violent extremist are used interchangeably. In a November 2020 report to Congress, the FBI and DHS jointly identified five domestic terrorism threat group categories, which, according to officials, help the FBI to better

---

[23]For example, it is a felony in Connecticut if a person maliciously, and with specific intent to intimidate or harass another person, causes physical injury to another person motivated by the actual or perceived *race, religion, ethnicity, disability, sex, sexual orientation or gender identity or expression* of such other person. Conn Gen. Stat. § 53a-181j (emphasis added). In Idaho, it is unlawful to maliciously and with the specific intent to intimidate or harass another person, cause physical injury, damage to real or personal property, or threaten by word or act because of that person's *race, color, religion, ancestry, or national origin*. Idaho Code § 18-7902 (emphasis added). In addition, some states have enacted sentencing enhancements that are applied where evidence of bias motivation is found in conjunction with underlying criminal acts. For example, an Alabama statute provides additional penalties for specified classes of convictions where it is shown that the perpetrator committing the underlying offense was motivated by the victim's actual or perceived race, color, religion, national origin, ethnicity, or physical or mental disability. Ala. Code § 13A-5-13. Furthermore, some states require law enforcement agencies within the state to collect data on hate crimes, which law enforcement agencies can subsequently, and on a voluntarily basis, report to FBI's UCR Program.

[24]According to DOJ, as of December 13, 2023, South Carolina and Wyoming do not have hate crime laws that cover protected categories identified in federal hate crime statutes.

[25]FBI and DHS, *Strategic Intelligence Assessment and Data on Domestic Terrorism* (Washington, D.C.: June 2023).

[26]According to DHS officials, DHS also considers violence in furtherance of political or social goals wholly or in part through unlawful acts of force or violence potentially destructive of critical infrastructure to constitute domestic violent extremism, consistent with DHS's statutory authorities under the Homeland Security Act of 2002, as amended.

understand criminal actors and help inform DHS's intelligence and threat prevention efforts.[27]

In addition, according to FBI and DHS' *Strategic Intelligence Assessment and Data on Domestic Terrorism* report, hate crimes and domestic terrorism incidents are not mutually exclusive. While there is no federal statute specifically criminalizing domestic terrorism, individuals who plan or carry out terrorist attacks may be federally prosecuted under a wide range of criminal statutes. For example, federal prosecutors can prosecute domestic terrorist incidents by bringing charges for firearms violations, interstate threats, or hate crimes when applicable.[28]

DOJ Roles and Responsibilities for Investigating and Prosecuting Hate Crimes

DOJ's FBI is the lead investigatory agency for all federal hate crime investigations. The FBI may work closely with state and local law enforcement agencies and other federal partners to investigate hate crimes and crimes motivated by bias, including in cases where federal charges are not brought. According to FBI documentation, the FBI provides law enforcement agencies with resources, forensic expertise, and experience in identification and proof of hate-based motivations to support agencies' investigations. According to FBI and DHS

---

[27]The five threat group categories include: (1) Racially or ethnically motivated violent extremism; (2) Anti-government or anti-authority violent extremism; (3) Animal rights/environmental violent extremism; (4) Abortion-related violent extremism; and (5) All other domestic terrorism threats. According to DHS officials, these threat group categories were initially agreed to during an August 2019 National Security Council Meeting. Pursuant to Section 5602(a), (b), and (d) of the National Defense Authorization Act for Fiscal Year (FY) 2020, the FBI and DHS—in consultation with the Office of the Director of National Intelligence, including the National Counterterrorism Center, and with DOJ—jointly produced four reports on domestic terrorism. See Pub. L. No. 116-92, § 5602(a)-(b), (d), 133 Stat. 1198, 2154 (2019). One report, *Domestic Terrorism: Definitions, Terminology, and Methodology*, published in November 2020, related to the standardization of terminology and procedures relating to domestic terrorism. The other three, titled *Strategic Intelligence Assessment and Data on Domestic Terrorism*, published in May 2021, October 2022, and June 2023, contained strategic intelligence assessments and data updates on domestic terrorism as of the end of 2019, for FY 2020 and FY2021, and for FY 2022, respectively.

[28]FBI and DHS' 2023 *Strategic Intelligence Assessment and Data on Domestic Terrorism* report notes that hate crime charges may be appropriate where individuals engage in domestic terrorism that is motivated by biases against a race, religion, ethnicity, or other specified factors. However, not all hate crimes cases involve domestic terrorism. FBI and DHS, *Strategic Intelligence Assessment and Data on Domestic Terrorism* (Washington, D.C.: June 2023).

documentation, the FBI created the Domestic Terrorism-Hate Crimes Fusion Cell in April 2019. It created the fusion cell to address the intersection of the FBI counterterrorism and criminal investigative missions to combat domestic terrorism and provide justice to those who are victims of hate crimes.[29] According to FBI officials, the fusion cell coordinates information sharing between DOJ's and FBI's hate crime and domestic terrorism investigative and prosecutorial components.

DOJ's Civil Rights Division and the 94 U.S. Attorneys' Offices share responsibility for prosecuting federal civil rights statutes, which include hate crimes. The Civil Rights Division is responsible for conducting, handling, and supervising civil rights cases. U.S. Attorneys' Offices assist the Civil Rights Division by providing additional resources to redress civil rights violations, knowledge of local dynamics in both investigations and litigation, and subject matter expertise in particular civil rights areas.

DOJ Data Collection Programs for Generating National Crime Statistics, including Hate Crimes

DOJ administers two statistical programs to measure the magnitude, nature, and impact of crime in the nation: the FBI's UCR Program and BJS' National Crime Victimization Survey. Each program, although complementary, is managed independently and for a specific purpose. Furthermore, each program collects data on a wide range of criminal activity and crime victimization, including but not limited to hate crimes.

FBI Uniform Crime Reporting Program. Since the passage of the Hate Crime Statistics Act in 1990, the FBI used its UCR Program to collect hate crime data from law enforcement agencies through the Summary Reporting System and National Incident-Based Reporting System (NIBRS).[30] However, in 2021, the FBI's UCR Program started to phase out the reporting of crime data from the Summary Reporting System in favor of a NIBRS-only data collection system. According to DOJ, NIBRS

---

[29]FBI and DHS, *Strategic Intelligence Assessment and Data on Domestic Terrorism* (Washington, D.C.: May 2021).

[30]See 34 U.S.C. § 41305. The UCR Program used the Summary Reporting System as a national method of collecting Uniform Crime Reporting statistics for the FBI since the 1930s. The FBI developed NIBRS in the 1980s to illustrate the volume, diversity, and complexity of crime more effectively than the original Summary Reporting System method. NIBRS is an incident-based reporting system in which agencies collect data on each single crime incident—as well as on separate offenses within the same incident—and was implemented to improve the overall quality of crime data collected by law enforcement.

is a significant shift—and improvement—in how the federal government measures and estimates reported crime. Compared to the Summary Reporting System, NIBRS collects data on 47 more offenses from participating law enforcement agencies and allows for the collection of more detailed data on the characteristics of criminal incidents, such as location of the crime; types and amount of property lost; and demographic information about the perpetrator(s) and victim(s).

While the Uniform Federal Crime Reporting Act of 1988 requires federal law enforcement agencies to report crime data to the UCR Program, reporting by state and local law enforcement agencies is voluntary.[31] For most nonfederal law enforcement agencies, the UCR data are compiled from state and local law enforcement incident reports transmitted to a centralized repository within their state (referred to as a state UCR Program). The state UCR Program then forwards the data to the FBI's national UCR Program. Law enforcement agencies in states that do not have a state program can submit their data directly to the FBI. According to the FBI, the purpose of the UCR Program is to support law enforcement agencies, communities, researchers, and public leaders so they can better understand and make well-informed decisions about crime and public safety.

BJS National Crime Victimization Survey. BJS' National Crime Victimization Survey is a nationally representative annual survey of about 240,000 persons in about 150,000 households. BJS uses the survey to produce estimates of the prevalence of nonfatal crimes both reported and not reported to the police.[32] The survey collects information from victims about personal crimes (e.g., violent crimes and personal theft/larceny) and household property crimes (e.g., burglary/trespassing). Survey respondents provide information about themselves (e.g., age, sex, race)

---

[31]34 U.S.C. § 41303(c)(2).

[32]The BJS' National Crime Victimization Survey defines "victimization" as a single victim or household that experienced a criminal incident. Criminal incidents are distinguished from victimizations in that one criminal incident may involve one or more victims. For violent crimes (rape/sexual assault, robbery, aggravated assault, and simple assault) and for personal theft/larceny, the number of victimizations is the number of victims of that crime. For crimes against households (burglary, trespassing, other theft, and motor vehicle theft), each crime is counted as having a single victim—the affected household.

and whether they experienced a victimization in the past six months.[33] In addition, BJS also administers supplemental surveys—or supplements—to capture more specific aspects of certain types of criminal victimization while preserving consistency with the main National Crime Victimization Survey. There are currently five active National Crime Victimization Survey supplements: (1) the Identity Theft Supplement, (2) the Police Public Contact Survey, (3) the School Crime Supplement, (4) the Supplemental Fraud Survey, and (5) the Supplemental Victimization Survey.[34]

DOJ Collects Some Data about Hate Crimes on the Internet from Law Enforcement, but Could Explore Options to Collect More Complete Information Through Its Crime Victim Survey

DOJ Collects Data from Law Enforcement on the Characteristics of Hate Crimes that Occur on the Internet

Prior to 2016, data from FBI's UCR Program could not specify the internet as a location for a crime. In 2016, the FBI adopted "cyberspace" as a location that law enforcement agencies could select in NIBRS to indicate

---

[33]For each victimization incident, the survey also collects information from the victim about the offender's characteristics (e.g., age, race and Hispanic origin, sex, and victim-offender relationship), characteristics of the crime (e.g., time and place of occurrence, use of weapons, nature of the injury, and economic consequences), reasons the crime was or was not reported to a law enforcement agency, and the victim's experience with the criminal justice system.

[34]In our prior work we used data from the National Crime Victimization Survey's School Crime Supplement—among other sources—to review hostile behaviors in K-12 schools, including bullying, harassment, hate speech and hate crimes, or other types of victimization like sexual assault and rape. See GAO- *K-12 Education: Students' Experiences with Bullying, Hate Speech, Hate Crimes, and Victimization in Schools*, GAO-22-104341 (Washington, D.C.: Nov. 24, 2021).

that a crime, including a hate crime, occurred on the internet.[35] The FBI added cyberspace as a location in NIBRS based on recommendations from the Criminal Justice Information Services Division Advisory Policy Board to track the emergence of crimes occurring on the internet.[36]

According to our analysis of FBI's UCR Program hate crime data from 2016 through 2021, the number of hate crimes that occurred on the internet, as reported by law enforcement agencies, increased year-to-year and accounted for less than 2 percent of the total number of hate crimes reported. See table 1 for more detail.[37]

Table 1: Number of Hate Crimes on the Internet Reported to the Federal Bureau of Investigation's (FBI) Uniform Crime Reporting (UCR) Program between January 2016 and December 2021

Year	Total hate crimes reported to FBI's UCR Program	Total hate crimes on the internet reported to FBI's UCR Program	Percentage identified as hate crimes on the internet
2016	6,121	4	0.07%
2017	7,329	13	0.18%
2018	7,181	23	0.32%
2019	7,347	39	0.53%
2020	8,909	116	1.30%

[35]According to the 2021 *NIBRS User Manual*, "cyberspace" is defined as "a virtual or internet-based network of two or more computers in separate locations which communicate either through wireless or wire connections." For the purposes of this report, we refer to crimes that occur in "cyberspace" as crimes that occur on the internet. To learn more about specific cases of hate crimes that occurred on the internet, we reviewed DOJ press releases that described federal hate crime charges and convictions. For example, in one press release issued in August 2019, a man was sentenced to 60 months in prison for threatening employees of an Arab civil rights nongovernmental organization focused on encouraging Arab Americans to participate in American political and civic life. The threats against the organization were based on bias against the employees' perceived race and national origin. The man sent over 700 emails to the organization's employees, culminating in five death threats in 2017. DOJ, *Virginia Man Sentenced To 60 Months In Prison For Committing Hate Crime By Threatening Employees Of The Arab American Institute*, 19-866 (Washington, D.C.: August 15, 2019).

[36]The Criminal Justice Information Services Advisory Policy Board is a federal advisory committee that recommends to the FBI Director general policy with respect to the philosophy, concept, and operational principles of various criminal justice information systems managed by the FBI's Criminal Justice Information Services Division, such as the FBI's UCR Program.

[37]FBI officials told us that the full calendar year data for 2022 would not be available until fall 2023.

Year	Total hate crimes reported to FBI's UCR Program	Total hate crimes on the internet reported to FBI's UCR Program	Percentage identified as hate crimes on the internet
2021	10,957	127	1.16%
Total	**47,844**	**322**	**0.67%**

Source: GAO analysis of FBI data. | GAO-24-105553

FBI's hate crime data also illustrate key aspects of hate crimes that occurred on the internet, such as what kind of bias motivated the hate crime, the type of offense committed, and the race of the offender.

Bias motivation. Within the UCR Program, bias motivation is used to indicate whether an offense was motivated by the offender's bias and, if so, what type of bias. According to the data, 29 of the 34 possible bias motivations were associated with hate crimes that occurred on the internet. From January 2016 through December 2021, the most commonly reported bias motivation for hate crimes on the internet was Anti-Black or African American.

Offense. The FBI's UCR Program collects information on 81 total offenses associated with crimes, including hate crimes. According to the data, 11 of the 81 possible offense categories were associated with hate crimes that occurred on the internet.[38] From January 2016 through December 2021, the most commonly reported offense category associated with hate crimes that occurred on the internet was intimidation.[39]

---

[38]Offense types associated with hate crimes that occur on the internet include, in alphabetical order: counterfeiting/forgery; extortion/blackmail; false pretenses/swindle/confidence game; hacking/computer invasion; identity theft; impersonation; intimidation; pornography/obscene material; simple assault; weapon law violations; and welfare fraud. Through NIBRS, law enforcement agencies may report to UCR up to ten offenses within a single incident, offering a more complete picture of crime occurrences than reporting from law enforcement agencies that historically submitted data to the FBI's UCR Program through the Summary Reporting System.

[39]According to the FBI's *Hate Crime Data Collection Guidelines and Training Manual*, "intimidation" is defined as unlawfully placing another person in reasonable fear of harm through the use of threatening words and/or other conduct without displaying a weapon or subjecting the victim to an actual physical attack, including stalking.

Offender race. The FBI also collects data on the race of offenders that commit hate crimes.[40] From January 2016 through December 2019, the most commonly reported offender race for hate crimes on the internet was White. However, from January 2020 through December 2021, the most commonly reported offender race was Unknown, followed by White.[41]

Appendix II compares the most commonly reported categories for bias motivation, offense type, and offender race associated with hate crimes on the internet to the most commonly reported categories associated with all other hate crimes reported by law enforcement agencies to FBI's UCR Program from January 2016 through December 2021.

FBI's UCR Program Data Collection Relies on Voluntary Hate Crime Reporting from Law Enforcement Agencies Using NIBRS

Nonfederal law enforcement agencies can voluntarily report incidents of hate crimes on the internet to the FBI's UCR Program if they are certified and transitioned to report crime data to NIBRS. Most state and local law enforcement agencies that are certified and transitioned to NIBRS submit monthly crime reports to a centralized repository within their state (referred to as a state UCR Program).[42] The state UCR Program then

---

[40]According to the FBI's *Hate Crime Data Collection Guidelines and Training Manual*, the FBI issued guidance on how law enforcement agencies should collect and maintain race and ethnicity data in response to standards for federal data on race released by the Office of Management and Budget in 1997. These standards have two categories for data on ethnicity and five minimum categories for data on race. The hate crime data we obtained from FBI's UCR Program includes one data point on offender(s) race, even if the incident involved more than one offender. According to the *2021 NIBRS User Manual*, reporting agencies should submit an additional report to the FBI's UCR Program if an investigation reveals the incident involved more than one offender.

[41]According to the 2021 *NIBRS User Manual*, the FBI's UCR Program captures data about each of the offenders in an incident (e.g., his/her age, sex, race, and ethnicity). If the reporting agency knows nothing about the offenders—i.e., no one saw the offenders, there were no suspects, and the number of offenders is unknown—then the agency should enter Unknown as the data value for that incident.

[42]According to FBI officials, as of March 2022, all 50 U.S. state UCR Programs, the District of Columbia, and Guam were certified and transitioned to report crime data to the FBI's UCR Program via NIBRS.

forwards the data to the FBI's national UCR Program.[43] According to FBI officials, as of calendar year 2016, 34 state UCR Programs were certified to report crime data to NIBRS.[44]

Our analysis indicates law enforcement agencies in two states (Michigan and Washington) reported data on hate crimes that occurred on the internet to FBI's UCR Program in 2016.[45] In comparison, according to FBI officials, as of calendar year 2021, 48 state UCR Programs were certified to report crime data to NIBRS.[46] Our analysis indicates that, in 2021, law enforcement agencies in 28 states reported data on hate crimes that occurred on the internet.[47] Figure 1 shows the range and levels of hate crimes that occurred on the internet that were reported to the FBI's UCR program by law enforcement agencies between January 2016 and December 2021, by state. For more information, see appendix III.

---

[43]According to FBI officials, law enforcement agencies are fully transitioned when NIBRS certification is granted by the FBI and the agencies begin submitting NIBRS data to the FBI's UCR Program. Once a state UCR program receives NIBRS certification from the FBI, the state UCR program is responsible for certifying agencies to submit NIBRS-only data, and assists local agencies within the state with the NIBRS transition.

[44]This number does not include the District of Columbia or U.S. territories.

[45]However, UCR Program data indicate that law enforcement agencies in all U.S. states and the District of Columbia, except for Hawaii, reported data on hate crimes, generally, to FBI's UCR Program in 2016.

[46]This number does not include the District of Columbia or U.S. territories.

[47]UCR Program data indicate that law enforcement agencies in all U.S. states, the District of Columbia, and Guam reported data on hate crimes, generally, to FBI's UCR Program in 2021.

Figure 1: Number of Hate Crimes that Occurred on the Internet Reported by Law Enforcement Agencies to the Federal Bureau of Investigation (FBI) by State, Between January 2016 and December 2021
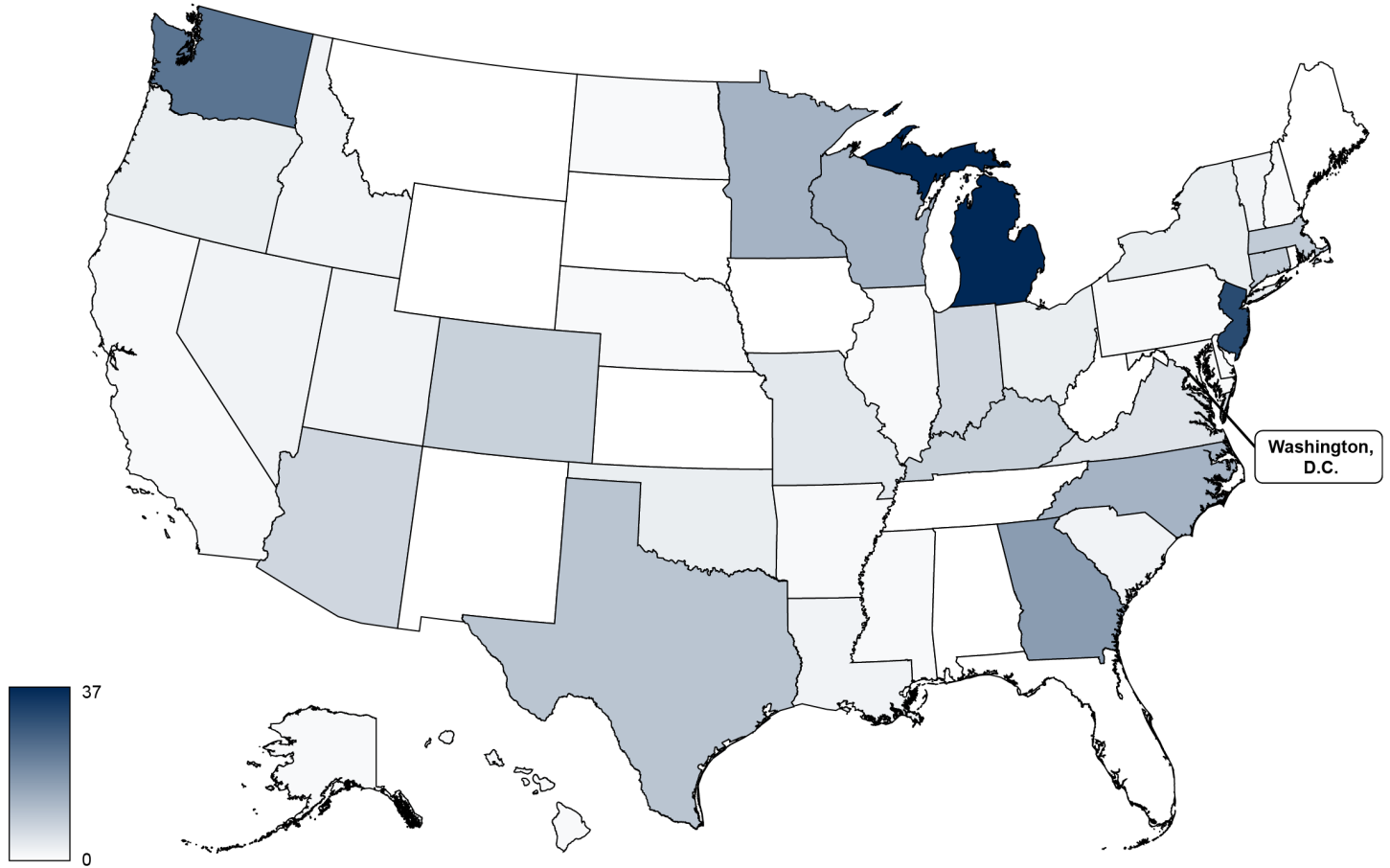
Source: GAO analysis of FBI's Uniform Crime Reporting Program data. | GAO-24-105553

Accessible Data Table for Figure 1: Number of Hate Crimes that Occurred on the Internet Reported by Law Enforcement Agencies to the Federal Bureau of Investigation (FBI) by State, Between January 2016 and December 2021

State	Hate Crimes that Occurred
Alabama	0
Arizona	7
Arkansas	1
California	1
Colorado	8
Connecticut	9
Delaware	1

State	Hate Crimes that Occurred
District of Columbia	0
Florida	0
Georgia	17
Idaho	2
Illinois	1
Indiana	7
Iowa	0
Kansas	0
Kentucky	8
Louisiana	2
Maine	0
Maryland	1
Massachusetts	9
Michigan	37
Minnesota	13
Mississippi	1
Missouri	4
Montana	0
Nebraska	1
Nevada	2
New Hampshire	1
New Jersey	31
New Mexico	0
New York	3
North Carolina	13
North Dakota	1
Ohio	3
Oklahoma	3
Oregon	3
Pennsylvania	1
Rhode Island	0
South Carolina	2
South Dakota	0
Tennessee	0
Texas	10
Utah	2

State	Hate Crimes that Occurred
Vermont	2
Virginia	5
Washington	24
West Virginia	0
Wisconsin	13
Wyoming	0
Alaska	1
Hawaii	1
Guam	1

Source: GAO analysis of FBI's Uniform Crime Reporting Program data. | GAO-24-105553

[a]State, local, tribal and university law enforcement agencies can voluntarily report hate crime data to the FBI's Uniform Crime Reporting Program. According to data we obtained from the FBI on the number of hate crimes that occurred on the internet from calendar years 2016 through 2021, law enforcement agencies in 12 states (Alabama, Florida, Iowa, Kansas, Maine, Montana, New Mexico, Rhode Island, South Dakota, Tennessee, West Virginia, and Wyoming) and the District of Columbia did not report any hate crimes that occurred on the internet during this time frame. This figure does not include data from U.S. territories.

In addition, according to our analysis of FBI data, as of 2021, approximately 69.8 percent of federal, state, and local law enforcement agencies across the country were certified and transitioned to NIBRS, up from 45.2 percent in 2016.[48] While all 50 state UCR Programs, the District of Columbia, and Guam were certified and transitioned to use NIBRS as of March 2022, not all local law enforcement agencies within the states were certified. According to FBI officials, since states vary in criminal codes and reporting requirements, states are responsible for NIBRS certification for local law enforcement agencies within each state. According to a DOJ report on the transition of law enforcement agencies to NIBRS, law enforcement agencies identified challenges impeding the transition, including (1) lack of available funding to procure a new records management system; (2) staff shortages that hinder data reporting; (3) local training insufficiencies that result in delays in NIBRS implementation and reporting; and (4) agency concerns that there will be a public perception that crime has significantly increased with the switch to NIBRS, since NIBRS captures more criminal offenses in a single incident

---

[48]Our analysis of FBI data includes the District of Columbia and U.S. territories.

than legacy reporting systems such as the Summary Reporting System.[49] Figure 2 illustrates the proportion of law enforcement agencies that were certified and transitioned to use NIBRS, by year.[50]

Figure 2: Percentage of Law Enforcement Agencies Nationwide[a] that were Certified and Transitioned to Use the National Incident-Based Reporting System (NIBRS)[b]
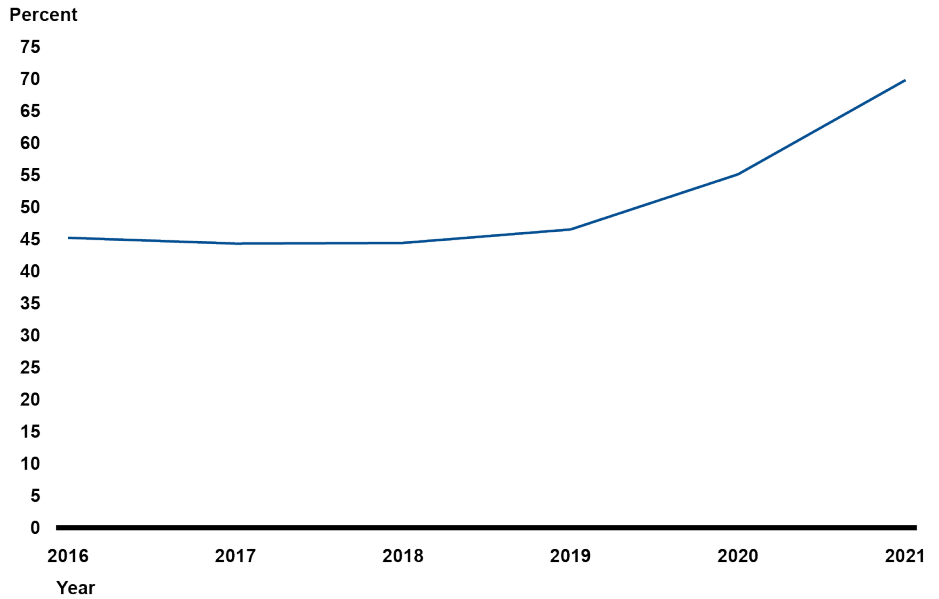
Source: GAO analysis of Federal Bureau of Investigation data. | GAO-24-105553

---

[49]According to the DOJ report, NIBRS can capture multiple criminal offenses that occur during a single incident unlike the Summary Reporting System which only allowed for the most serious offense to be collected. As a result, an increase in offenses is expected when agencies transition to NIBRS. According to the report, the FBI addressed these concerns with a study that analyzed the effects of NIBRS reporting on offense levels and showed only a nominal (2.4 percent) increase in crime reported via NIBRS in 2019. For further information, see DOJ, *Department of Justice Review of the Transition of Law Enforcement Agencies to the National Incident-Based Reporting System (NIBRS)* (Washington, D.C.: 2023).

[50]Currently, law enforcement agencies can report hate crimes that occurred on the internet to the FBI if the law enforcement agency is certified and transitioned to NIBRS. Specifically, law enforcement agencies cannot report hate crimes that occur on the internet to the FBI's UCR Program if the law enforcement agencies collect crime data through the Summary Reporting System.

Accessible Data Table for Figure 2: Percentage of Law Enforcement Agencies Nationwide[a] that were Certified and Transitioned to Use the National Incident-Based Reporting System (NIBRS)[b]

Year	Percentage
2016	45.2
2017	44.3
2018	44.4
2019	46.5
2020	55.1
2021	69.8

Source: GAO analysis of Federal Bureau of Investigation data. | GAO-24-105553

[a]For state, local, tribal and university law enforcement agencies, reporting crime data to the Federal Bureau of Investigation's (FBI) Uniform Crime Report (UCR) Program is voluntary. However, to report data on hate crimes that occur on the internet to the UCR, agencies must become certified and transitioned to use NIBRS.

[b]According to FBI data, although the total number of law enforcement agencies that were certified and transitioned to use NIBRS increased year to year from calendar years 2016 through 2021, the total number of law enforcement agencies nationwide varied from year to year. This variation accounts for the fluctuation in the percentage of law enforcement agencies nationwide that were certified and transitioned as presented in the graph. For example, in 2016 the total number of law enforcement agencies was 18,631; from 2017 through 2020, the number of law enforcement agencies totaled around 20,200 agencies; in 2021, the number increased to 20,630. According to a 2023 Department of Justice (DOJ) report, various factors, such as funding, staff resources, or training, can affect whether a law enforcement agency becomes certified and transitioned to use NIBRS. DOJ, *Department of Justice Review of the Transition of Law Enforcement Agencies to the National Incident-Based Reporting System (NIBRS)*, (Washington, D.C.: 2023).

DOJ is Working with Law Enforcement Agencies to Address Limitations in Hate Crime Reporting

Nongovernmental organizations we interviewed said limitations exist about hate crime data reported to the FBI's UCR Program, but DOJ officials said they are working to address those limitations. According to all three nongovernmental organizations we spoke with about FBI's UCR Program, FBI's data on hate crimes, including hate crimes on the internet, are limited due to a number of factors. These factors include: 1) the absence of a requirement for non-federal law enforcement agencies to report crime data to the FBI; 2) hate crimes are under-investigated and under-prosecuted because, in part, it is difficult for local law enforcement agencies to prove an offender's bias motivation, especially in situations involving the internet since offenders on the internet are often anonymous; and 3) several communities targeted by hate crimes distrust law enforcement, therefore individuals are hesitant to report incidents.

To help improve hate crime data reporting to the FBI, DOJ officials told us that they assist state and local law enforcement agencies transitioning to NIBRS by engaging with these agencies directly and by providing multiple funding opportunities. For example, in 2021 and 2022, the FBI organized six regional conferences for law enforcement agencies, including agencies that the FBI identified had not reported or had underreported hate crimes. The conferences involved raising awareness about federal hate crime laws, discussing best practices for collaboration between federal and local law enforcement agencies to investigate these crimes, and providing training on transitioning to and reporting crime data using NIBRS.

Furthermore, according to FBI officials, the FBI is assisting 27 local law enforcement agencies representing the nation's largest populations such as New York City, Los Angeles, and Miami to transition to NIBRS, by providing technical expertise, data integration, and subject matter support, along with no-cost training. Additionally, through BJS, the National Crime Statistics Exchange initiative provides funding and other resources to state and local law enforcement agencies to support the expansion of NIBRS reporting.[51] According to DOJ officials, as of August 2022, DOJ has awarded approximately $120 million to 120 local law enforcement agencies and state UCR programs—including 40 of the nation's 72 largest law enforcement agencies—to implement NIBRS. According to FBI officials, 33 of these 40 agencies that received funding have successfully transitioned to NIBRS as of August 2022. Furthermore, the National Institute of Justice funds research and evaluation projects to

---

[51]The National Crime Statistics Exchange initiative is designed to: (1) coordinate information sharing among state and local law enforcement agencies, state UCR Programs, the law enforcement technology industry, and other key stakeholders, (2) provide guidance to transitioning agencies, and (3) promote efficient and economical practices including the adoption of new technologies or software for agencies to report crime data through NIBRS. BJS is authorized to "make grants to, or enter into cooperative agreements or contracts with, public agencies, institutions of higher education, private organizations, or private individuals" for purposes of collecting and analyzing criminal justice statistics. 34 U.S.C. § 10132(c)(1). This authority was identified in various NIBRS transition-related grant funding solicitations issued by BJS. *See e.g.* BJS, *2017 NCS-X Implementation Assistance Program: Phase V- Support for Large Local Agencies* (May 16, 2017). Similarly, the Jabara-Heyer NO HATE Act authorizes BJS to provide funding and technical assistance to increase the number of local law enforcement agencies reporting data to NIBRS. 34 U.S.C. § 30507(d); *see e.g.* BJS, *FY 2023 Law Enforcement Transition to the National Incident-Based Reporting System (NIBRS) to Improve Hate Crime Reporting* (June 1, 2023).

develop evidence to inform efforts to prevent and combat hate crimes and their effects, such as how hate crime reporting may be improved.[52]

To help improve law enforcement agencies' responsiveness to hate crimes, DOJ provides multiple funding opportunities to support hate crime investigations and prosecutions. For example, DOJ's Office of Justice Programs funds efforts by state and local law enforcement and prosecution agencies and their partners to investigate and prosecute hate crimes.[53] Moreover, in addition to supporting the expansion of NIBRS reporting, BJS' National Crime Statistics Exchange initiative also provides funding and technical expertise to law enforcement agencies. For example, the initiative supports hate crimes training and funding to adopt new technologies—such as new records management systems—that support the investigation and reporting of hate crimes using NIBRS.

The FBI collaborates with local and state law enforcement agencies to investigate federal hate crimes, including those that occur on the internet. We spoke with six federal, state, and local law enforcement agencies to determine whether the agencies experienced any challenges with investigating hate crimes and reporting such data to the FBI's UCR Program.[54] Each of the five state and local law enforcement agencies we spoke with said they collaborate with the FBI to investigate hate crimes that occur on the internet, such as by referring cases to their FBI counterparts if the crime involves perpetrators located outside of the law

---

[52]For example, the National Institute of Justice solicited applications for a 2023 grant program aimed at rigorous research and evaluation projects that inform efforts to prevent and combat hate crimes and their effects. Specifically, the program solicited proposals to advance knowledge and understanding in the following two categories: (1) preventing and addressing hate crimes; and (2) school-based hate crimes. National Institute of Justice, *NIJ FY23 Research and Evaluation on Hate Crimes* (February 28, 2023); Pub. L. No. 111-84, § 4704, 123 Stat. 2190, 2837 (2009) (authorizing the Attorney General to award grants to State, local, and tribal law enforcement agencies for extraordinary expenses relating to the investigation or prosecution of hate crimes).

[53]DOJ's Bureau of Justice Assistance's Matthew Shepard and James Byrd, Jr. Hate Crimes Program supports state, local, and tribal law enforcement and prosecution agencies and their partners in conducting outreach, educating practitioners and the public, enhancing victim reporting tools, and investigating and prosecuting hate crimes committed on the basis of a victim's perceived or actual race, color, religion, national origin, sexual orientation, gender, gender identity, or disability. § 4704, 123 Stat. at 2837; *see e.g.* Bureau of Justice Assistance, *BJA FY21 Matthew Shepard and James Byrd, Jr. Hate Crimes Program* (May 14, 2021).

[54]We selected agencies to interview based on a variety of factors that included variation in geographic dispersion, population size of the agency's jurisdiction, agency type (such as federal, state, city, county, or university), and the extent to which they reported data on hate crimes that occurred the internet between 2016 and 2020 to FBI's UCR Program.

enforcement agency's jurisdiction. Officials from one state UCR Program we spoke with said they collaborate with the FBI on a daily basis to review hate crime incident data reported to the state and forwarded to the FBI. Furthermore, officials from four of the six federal, state, and local law enforcement agencies we spoke with said there were no major challenges with identifying or investigating hate crimes that occur on the internet or reporting such crimes to the FBI's UCR Program.

To help improve victims' reporting of hate crimes to law enforcement agencies, DOJ offers programming to engage the public on the importance of reporting such crimes. For example, DOJ created the United Against Hate Community Outreach Program which aims to build trust between law enforcement agencies and the communities they serve to better identify, report, and prevent acts of hate. DOJ implemented the program in all 94 U.S. Attorneys' Offices across the country. In addition, DOJ's Bureau of Justice Assistance funds efforts by state and local law enforcement agencies and prosecutors to conduct outreach to and education of the public, victims, and partner agencies on hate crimes.[55] Furthermore, in 2021 DOJ established an Anti-Hate Crimes Resources Coordinator to lead DOJ's efforts to eradicate hate crimes through training, outreach, and education for law enforcement and the public at the federal, state, and local levels.

DOJ Does Not Collect Data about Hate Crimes on the Internet from Its Crime Victimization Survey

DOJ—through BJS—collects data from U.S. households about bias-motivated victimization through its National Crime Victimization Survey. In 2003, BJS began collecting these data in the National Crime Victimization Survey by asking survey respondents if they experienced a victimization that they suspected was motivated by bias against them because of their actual or perceived race, religion, gender, ethnic background or national origin, sexual orientation, or disability. In the current version of the survey instrument, as of September 2023, for a victimization incident to be classified as a hate crime, victims must report at least one of the following types of evidence: (1) confirmed by law enforcement as bias-motivated, according to the victim's report; (2) perceived by victims to be bias-motivated because the offender(s) used hate language; or (3) perceived by victims to be bias-motivated because the offender(s) left behind hate

---

[55]§ 4704, 123 Stat. at 2837; *see e.g.* Bureau of Justice Assistance, *BJA FY21 Matthew Shepard and James Byrd, Jr. Hate Crimes Program* (May 14, 2021).

symbols.[56] In addition to measuring bias-motivated victimization in the core National Crime Victimization Survey, one of the survey's supplements—the School Crime Supplement—measures whether students ages 12 to 18 experienced or witnessed bias-motivated victimization at school.[57]

However, the National Crime Victimization Survey does not currently capture victimization that occurs on the internet in the core survey. BJS officials told us the National Crime Victimization Survey was not historically designed to collect information about criminal victimization that occurred on the internet. For example, threats must be made face to face to be classified as a crime in the survey according to BJS officials. In addition, BJS officials told us that measuring crimes that occur on the internet in the National Crime Victimization Survey presents unique challenges that require additional research and testing, such as examining whether survey respondents would be able to accurately respond to questions about the motivation for a crime on the internet.

In May 2022, Congress passed the Better Cybercrime Metrics Act, which directs DOJ to enter into an agreement with the National Academy of Sciences to develop a classification system for categorizing different types of crimes that occur on the internet.[58] Furthermore, the act requires the Director of BJS, in coordination with the Director of the U.S. Bureau of the Census, to include questions relating to cybercrime victimization in

---

[56]BJS uses the Hate Crime Statistics Act to define a hate crime. See 34 U.S.C. § 41305.

[57]In our prior work we used data from National Crime Victimization Survey's School Crime Supplement—among other sources—to review hostile behaviors in K-12 schools, including bullying, harassment, hate speech and hate crimes, or other types of victimization like sexual assault and rape. See GAO, *K-12 Education: Students' Experiences with Bullying, Hate Speech, Hate Crimes, and Victimization in Schools*, GAO-22-104341 (Washington, D.C.: Nov. 24, 2021).

[58]Pub. L. No. 117-116, § 3, 136 Stat. 1180, 1180-81. In passing the law, Congress found, among other things, that public polling indicates that cybercrime could be the most common crime in the United States and that the United States lacks comprehensive cybercrime data and monitoring. § 2, 136 Stat. at 1180. For additional information on how federal agencies have responded to the Better Cybercrime Metrics Act, including DOJ, see GAO, *Cybercrime: Reporting Mechanisms Vary, and Agencies Face Challenges in Developing Metrics*, GAO-23-106080 (Washington, D.C.: June 20, 2023).

the National Crime Victimization Survey.[59] The Better Cybercrime Metrics Act does not explicitly mandate BJS to capture whether bias was a motivating factor for victimization that occurred online.

However, as of April 2023, BJS officials said they were conducting research on the types, definitions, and measurement of victimization that occurs on the internet, and said additional research is necessary to collect information on whether bias was a motivating factor for a crime that occurred on the internet. For example, BJS officials told us that the majority of hate crimes captured by the National Crime Victimization Survey from 2015 through 2019 involved physical confrontations—simple assault (62 percent) and aggravated assault (18 percent)—that cannot occur on the internet. Related to this effort, in August 2023, BJS published a third-party report that described information on the types, definitions, and measurement of cybercrime and examined various approaches for how the National Crime Victimization Survey could measure cybercrimes.[60] The report examined whether BJS could use the School Crime Supplement's approach to measuring bias-motivated bullying on the internet to also measure bias-motivated cybercrimes, but the report did not recommend using that method. However, the report did not explore other methods to measure bias-motivated cybercrimes, such as using a similar approach to how the National Crime Victimization Survey classifies an in-person victimization as a hate crime. As BJS officials stated, BJS would need to conduct additional research and testing to expand the survey to measure bias-motivated cybercrimes. However, officials did not provide information on when BJS plans to pursue such additional research and testing.

According to FBI and BJS officials, using data collected by both the National Crime Victimization Survey and the FBI's UCR Program can

[59]The Act authorized the appropriation of $1 million for the National Academy of Sciences project and $2 million for the incorporation of questions relating to cybercrime victimization in the National Crime Victimization Survey. §§ 3, 5, 136 Stat. at 1180-81. In DOJ's FY 2024 Congressional Budget Submission, BJS requested $2 million for a new data collection on cybercrime metrics in response to requirements in the Better Cybercrime Metrics Act. Such funds and staff allocation are to (a) research and test the most appropriate method to comply with the law while preserving the integrity of the National Crime Victimization Survey, (b) implement the methods that are selected, and (c) analyze and report any data collected on cybercrime victimization. BJS officials stated that, as of December 2023, the funding has not been appropriated.

[60]Julia Brinton, Lynn Langton, Christopher Krebs, and Michelle Casper, *An Environmental Scan of Cybercrime Measurement: Recommendations for the National Crime Victimization Survey*, NCJ 306766 (Research Triangle Park, North Carolina: RTI International, August 2023).

jointly provide a greater understanding of crime trends and the nature of crime in the U.S. Furthermore, according to FBI and BJS officials, the complementary information each data source produces provides a more comprehensive understanding of national crime levels than either could produce alone. For example, according to our analysis of hate crime data from FBI's UCR Program, law enforcement agencies reported 7,347 hate crimes to the FBI in 2019. In contrast, according to a BJS report, BJS' National Crime Victimization Survey data estimated that U.S. residents experienced approximately 305,390 bias-motivated victimizations in 2019.[61]

The report states that differences in hate crime numbers estimated by the National Crime Victimization Survey and those produced by the FBI's UCR Program can largely be attributed to two factors: (1) victims' reporting and (2) law enforcement classification of reported crimes as hate crimes. Victims may not report all incidents of victimization to law enforcement agencies. In addition, the report states that differences in the numbers could be due to various factors impacting the ability of law enforcement agencies to classify a reported crime as a hate crime, such as the availability of sufficient evidence upon investigation of the reported crime to classify it as a hate crime. According to the report, because the BJS' National Crime Victimization Survey and the FBI's UCR Program measure an overlapping, but not identical, set of offenses, complete congruity should not be expected between hate crime estimates from these two sources.

While the FBI collects data from law enforcement agencies on hate crimes that occur on the internet, BJS does not capture similar data on bias-motivated victimization that occurs on the internet through the National Crime Victimization Survey. The absence of methods to measure bias-motivated criminal victimization on the internet in the National Crime Victimization Survey limits DOJ's ability to more readily produce a comprehensive understanding of national crime levels.

Standards for Internal Control in the Federal Government states that obtaining and using quality information helps agencies make informed

---

[61]Grace Kena and Alexandra Thompson, *Hate Crime Victimization, 2005–2019, 2021 Edition,* NCJ 300954 (Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, 2021).

decisions and evaluate performance in achieving key objectives.[62] According to DOJ's Fiscal Years 2022-2026 Strategic Plan, DOJ plans to improve hate crime incident reporting by working with federal agencies, stakeholders, and Congress. The plan states DOJ will develop policies, programs, legislation, regulatory action, research, and grant-making to strengthen federal civil rights outreach, enforcement, and coordination. Furthermore, the Plan states DOJ will continue to combat unlawful acts of hate, including by improving incident reporting—which could include the collection of more complete victimization data. Through these steps, the Plan states DOJ will be better positioned to deter hate crimes, address them when they occur, support those who are victimized, and reduce the pernicious effects of these crimes on our society.

In addition to the goals outlined in the Strategic Plan about improving incident reporting, DOJ's Anti-Hate Crimes Resources Coordinator told us that collecting better data about victimization could help identify communities that underreport hate incidents and improve DOJ's efforts to allocate prevention resources. As BJS continues to research ways to implement requirements mandated by the Better Cybercrime Metrics Act, exploring options to measure bias-related criminal victimization that occurs on the internet in the National Crime Victimization Survey—or in one of its supplements—would improve DOJ's tracking of all hate crimes and complement data collected from law enforcement agencies. In addition, collecting such information could assist federal, state, and local governments as they plan and prioritize their efforts to prevent and combat hate crimes in their communities.

---

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

Selected Companies Took Varied Steps to Remove Some Hate and Violent Extremist Speech on Their Internet-based Platforms

Six selected companies that operate seven different internet-based platforms removed differing amounts of content or numbers of users that violated their hate and violent extremist speech policies.[63] The data reflect the amount of enforcement action companies with publicly available enforcement policies took against violative content.[64] These companies varied in their overall number of users and in their hate speech and violent extremist speech policies, including how they enforce the policies. Although enforcement data we analyzed do not measure the total extent of hate speech or violent extremist speech, these data represent the

---

[63]The seven platforms comprise four social media platforms, one livestreaming and media-hosting platform, one communication and messaging platform, and one crowdfunding and financial transaction platform. We selected companies whose platforms were the most-cited in studies and news articles, across a range of different types of services provided by internet-based platforms. We reviewed whether the companies' publicly available policies explicitly prohibited hate speech or violent extremist speech on their platforms. We analyzed enforcement data from companies in six-month time periods—January through June and July through December—when complete data were available between January 2018 and December 2022. For more detailed information on scope and methodology, see Appendix I.

[64]Companies may use community guidelines, policies, and terms of service to define what users are prohibited from doing—such as defining types of prohibited text, images, and audio (i.e., violative content)—on the companies' platforms. For the purposes of this report, we refer to these collectively as policies. Our review of companies' hate speech and violent extremist speech policies showed that the titles of the policies varied, but generally prohibited the same types of conduct or behavior. Companies' hate speech policies prohibited direct attacks against people or groups based on various characteristics such as race, religion, disability, or sexual orientation, among others. Prohibited content included speech that dehumanizes people or groups by comparing them to animals, insects, pests, or diseases; speech using hateful slurs; speech calling for violence, exclusion, segregation, or discrimination; speech claiming people or groups are physically, mentally, or morally inferior; speech denying historical events such as the Holocaust; and the use of hateful symbols or imagery, such as swastikas. Similarly, companies' violent extremist speech policies prohibited content that promoted violent extremist, terrorist, or criminal organizations or individuals, including hateful organizations that dehumanize, incite hate or violence toward, or promote hateful ideologies against people or groups based on various characteristics such as those listed in their hate speech policies. Violent extremist speech could include content justifying or praising such organizations' violent acts, recruiting new members, or promoting the organizations' insignias or symbols.

---

amount of content or the number of users each company identified that violated their hate speech or violent extremist speech policies.

Enforcement of Hate Speech Policies

Each of the six selected companies had hate speech policies and related enforcement data for the seven internet-based platforms they operate. According to our analysis of these companies' publicly available policies, there are 17 characteristics covered by hate speech policies, including, for example those related to race, gender, and age. See Figure 3.

Figure 3: Protected Characteristics Explicitly Mentioned in Hate Speech Policies for Seven Selected Internet-based Platforms
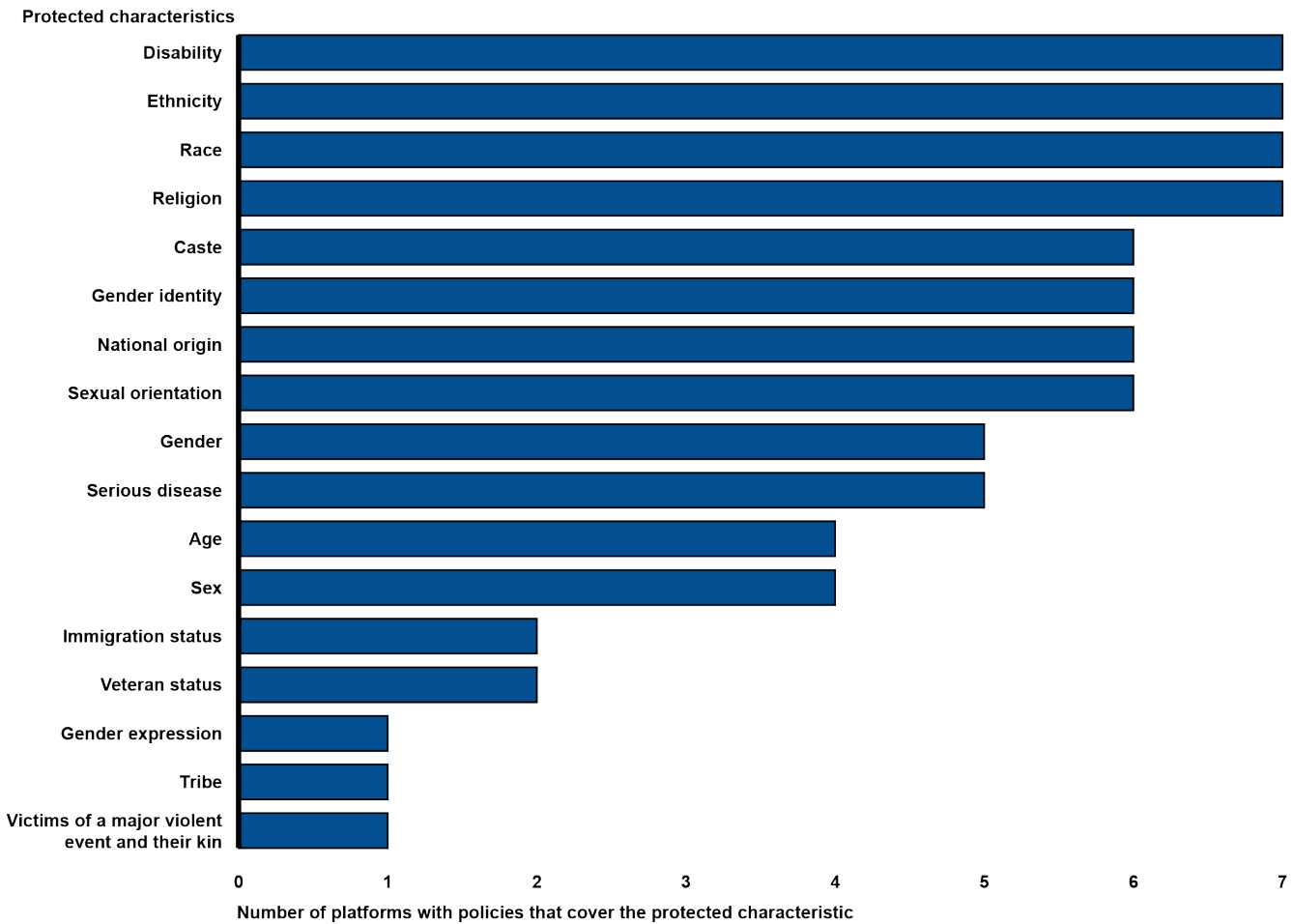
Source: GAO analysis of hate speech policies from selected companies that operate internet-based platforms. | GAO-24-105553

Accessible Data Table for Figure 3: Protected Characteristics Explicitly Mentioned in Hate Speech Policies for Seven Selected Internet-based Platforms

Protected Characteristics	Number of Platforms
Disability	7
Ethnicity	7
Race	7
Religion	7
Caste	6
Gender identity	6
National origin	6
Sexual orientation	6
Gender	5
Serious disease	5
Age	4
Sex	4
Immigration status	2
Veteran status	2
Gender expression	1
Tribe	1
Victims of a major violent event and their kin	1

Source: GAO analysis of hate speech policies from selected companies that operate internet-based platforms.. | GAO-24-105553

Social media platforms. The four social media platforms varied in the amount of violative content removed year-to-year. For example, on two social media platforms, the most violative content was removed from January 2021 through June 2021, then less violative content was removed in the following 18 months through December 2022. For another social media platform, more violative content was removed from July 2022 through December 2022 than in prior years. Figure 4 shows the amount of content the four social media platforms removed for violating their hate speech policies.[65]

---

[65]For the purposes of this report, references to company platforms by anonymized names (e.g. "social media platform 1") are consistent throughout the report. According to officials from a company that operates one of the four social media platforms, violative hate speech content from the U.S. represented about 39 percent of violative hate speech content globally from October 2022 through December 2022.

Figure 4: Trends in the Amount of Content Removed on Selected Social Media Platforms for Violations of their Hate Speech Policies[a]

Counts of content removed (in millions)

Source: GAO analysis of enforcement data from selected companies that operate internet-based platforms. | GAO-24-105553

Accessible Data Table for Figure 4: Trends in the Amount of Content Removed on Selected Social Media Platforms for Violations of their Hate Speech Policies[a]

	Counts of content removed (in millions)			
Date	Social Media Platform 1	Social Media Platform 2	Social Media Platform 3	Social Media Platform 4
2018 Jan.-June	5			
2018 July-Dec.	6.3			0.661329
2019 Jan.-June	8.3			2.4817
2019 July-Dec.	12.4			1.44547
2020 Jan.-June	32	3.7776	0.83635	0.955212
2020 July-Dec.	49	13.1	1.78266	1.62828
2021 Jan.-June	56.7	16.1	3.21828	1.60698
2021 July-Dec.	39.7	9.8	2.68404	1.29318
2022 Jan.-June	28.6	7.2	3.57165	1.52844
2022 July-Dec.	21.6	9	4.18975	

Source: GAO analysis of enforcement data from selected companies that operate internet-based platforms.. | GAO-24-105553

[a]These data reflect global enforcement of hate speech policies on the social media platforms.

Livestreaming and media-hosting platform. For the selected company in our review that operated a livestreaming and media-hosting platform, progressively more violative content was removed across the January 2019 to December 2022 time frame. Figure 5 shows the amount of content the platform removed for violating its hate speech policy.

Figure 5: Trend in the Amount of Content Removed on a Selected Livestreaming and Media-hosting Platform for Violations of Its Hate Speech Policy[a]

Counts of content removed (in thousands)
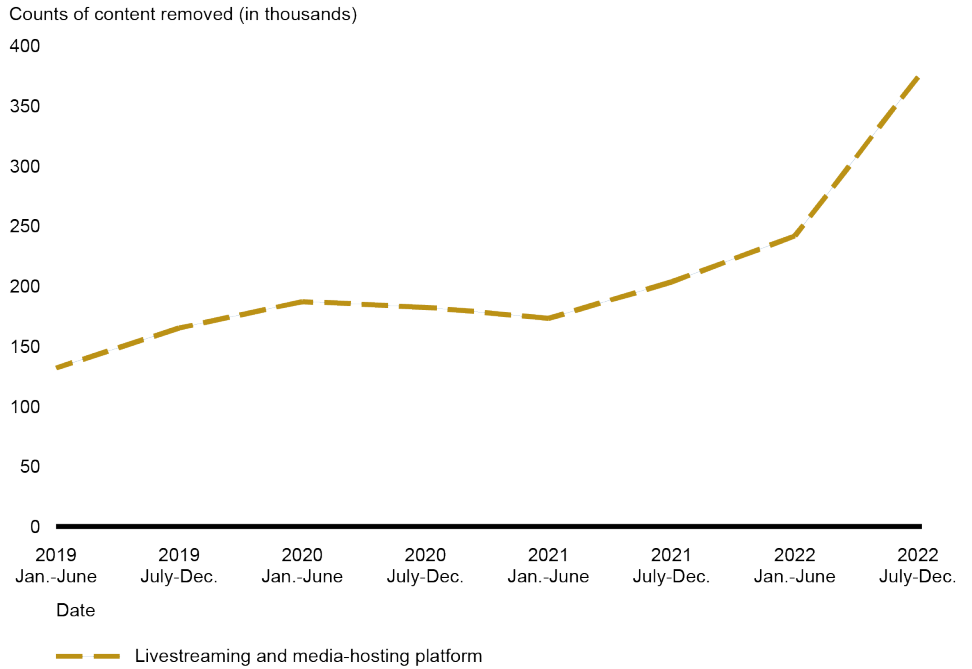
Source: GAO analysis of enforcement data from a selected livestreaming and media-hosting platform. | GAO-24-105553

Accessible Data Table for Figure 5: Trend in the Amount of Content Removed on a Selected Livestreaming and Media-hosting Platform for Violations of Its Hate Speech Policy[a]

Date	Counts of Content removed (in thousands)
2019 Jan.-June	131.887
2019 July-Dec.	165.203
2020 Jan.-June	187.207
2020 July-Dec.	182.496
2021 Jan.-June	173.19
2021 July-Dec.	203.532
2022 Jan.-June	241.635
2022 July-Dec.	373.825

Source: GAO analysis of enforcement data from a selected livestreaming and media-hosting platform. | GAO-24-105553

[a]These data reflect global enforcement of the hate speech policy on the livestreaming and media-hosting platform.

Communication and messaging platform. Based on reports of potential hate speech policy violations to the company by U.S. users in 2022, more warnings were issued and users removed on the communication and messaging platform from January through June (3,429 total) than from July through December (2,584 total).

Crowdfunding and financial transaction platform. According to an official from a company that operates a crowdfunding and financial transaction platform, from 2018 through 2022 one crowdfunding campaign in 2021 violated the company's hate speech policy.[66]

Enforcement of Violent Extremist Speech Policies

Of the six companies we selected for review, five companies had policies that explicitly prohibit violent extremist speech, which includes the promotion of violent extremist groups or violent extremism against people based on protected characteristics.

Social media platforms. The four selected social media platforms had policies prohibiting violent extremist speech. On three social media platforms, more violative content was removed in 2022 than in prior years. Figure 6 shows the amount of violent extremist content that the three social media platforms took action against for violating their violent extremist speech policies.[67] The fourth social media platform collects data on users removed rather than content removed. On that platform, more users were removed in January through June 2019 than in the following years.

---

[66]These data reflect global enforcement of the company's hate speech policy.

[67]According to officials from one company, violative violent extremist speech from the U.S. represented nearly 11 percent of violative violent extremist speech globally from October 2020 through December 2022.

Figure 6: Trends in the Amount of Content Removed on Selected Social Media Platforms for Violations of their Violent Extremist Speech Policies[a]

Counts of content removed (in millions)

Date

— Social media platform 1   – – – Social media platform 2   •••••• Social media platform 3
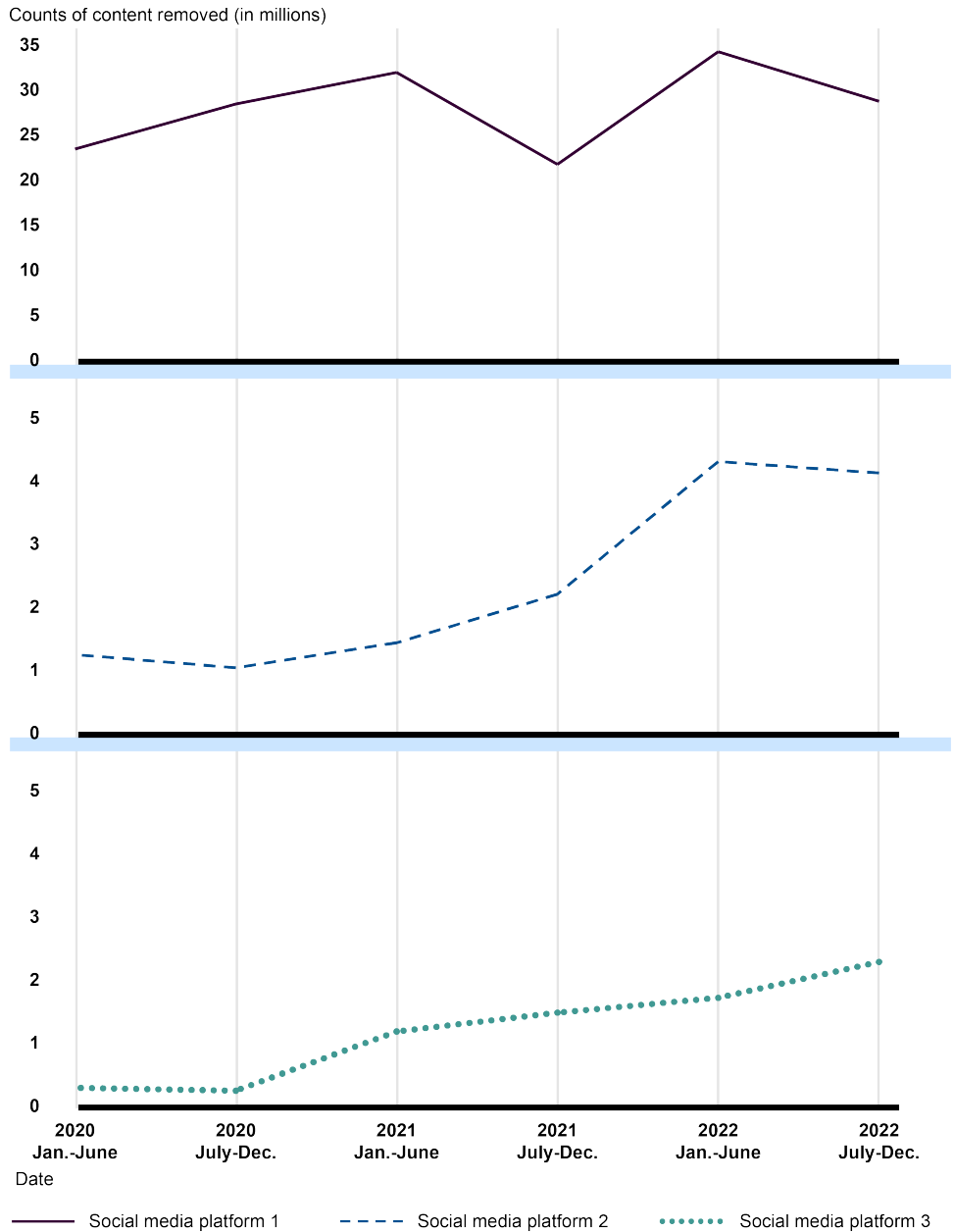
Source: GAO analysis of enforcement data from selected companies that operate internet-based platforms. | GAO-24-105553

Accessible Data Table for Figure 6: Trends in the Amount of Content Removed on Selected Social Media Platforms for Violations of their Violent Extremist Speech Policies[a]

Date	Counts of content removed (in millions)		
	Social Media Platform 1	Social Media Platform 2	Social Media Platform 3
2020 Jan.-June	23.6	1.2709	0.313631
2020 July-Dec.	28.6	1.0618	0.267399
2021 Jan.-June	32.1	1.4581	1.20646
2021 July-Dec.	21.9	2.2288	1.50473
2022 Jan.-June	34.4	4.3313	1.74042
2022 July-Dec.	28.9	4.1492	2.30908

Source: GAO analysis of enforcement data from selected companies that operate internet-based platforms. | GAO-24-105553

[a]These data reflect global enforcement of violent extremist speech policies on three social media platforms.

Livestreaming and media-hosting platform. On the livestreaming and media hosting platform, the amount of violent extremist content removed peaked during the January 2020 through June 2020 time period and by the end of 2022 declined overall back to the levels of content removed in 2019, as shown in Figure 7.

Figure 7: Trend in the Amount of Content Removed on a Selected Livestreaming and Media-hosting Platform for Violations of Its Violent Extremist Speech Policy[a]

Counts of content removed (in thousands)

Livestreaming and media-hosting platform
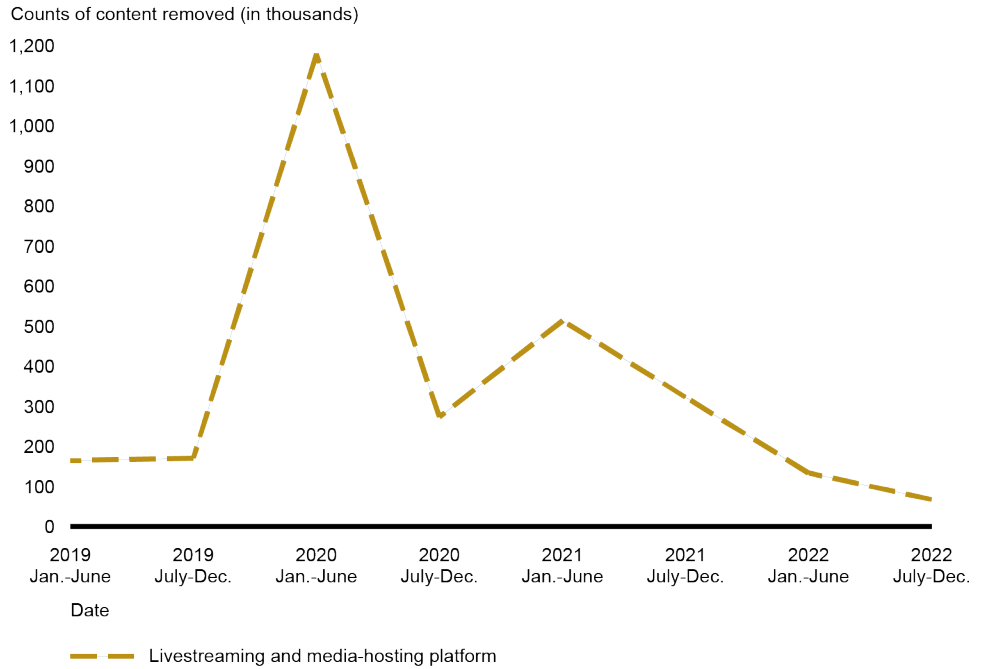
Source: GAO analysis of enforcement data from a selected livestreaming and media-hosting platform. | GAO-24-105553

Accessible Data Table for Figure 7: Trend in the Amount of Content Removed on a Selected Livestreaming and Media-hosting Platform for Violations of Its Violent Extremist Speech Policy[a]

Date	Counts of Content Removed (in thousands)
2019 Jan.-June	164.623
2019 July-Dec.	170.722
2020 Jan.-June	1180.69
2020 July-Dec.	273.475
2021 Jan.-June	513.908
2021 July-Dec.	322.751
2022 Jan.-June	133.711
2022 July-Dec.	67.516

Source: GAO analysis of enforcement data from a selected livestreaming and media-hosting platform. | GAO-24-105553

[a]These data reflect global enforcement of the violent extremist speech policy on the livestreaming and media-hosting platform.

Communication and messaging platform. Based on reports of potential violent extremist speech policy violations to the company by

U.S. users in 2022, more warnings were issued and users removed on the communication and messaging platform from July through December (81) than from January through June (67).

Selected Companies Continually Update Hate Speech and Violent Extremist Speech Policies and Associated Enforcement Mechanisms

Officials from the six selected companies we interviewed said they continually update their policies to, for example, reflect new developments in hate speech and violent extremist speech that appear on their platforms or to clarify what would be considered violative content. For example, one company amended its hate speech policy to forbid speech that compares people of certain races and religions to animals. Another company amended its hate speech policy to forbid the promotion of Nazism or the denial of well-documented events such as the Holocaust.

Furthermore, officials from all six companies we spoke with said they use algorithms to varying degrees to enforce policies against violative content. According to an official from one company, an algorithm automatically removes violative words from posted content.[68] According to officials from three other companies, using algorithms to detect potentially violative content is the only way they can review large amounts of uploaded content. Based on available data related to algorithmic enforcement, for three social media platforms, the algorithms, rather than platform users, generally identified the greatest proportion of content that was removed for violating the platforms' hate speech policies and violent extremist speech policies. From July through December 2022, the three selected social media platforms used algorithms that flagged 80 to 90 percent of all content removed for violating such policies.

Some company officials also stated that the companies continuously refine their algorithms to more accurately identify violative content. According to officials from three companies, human moderators constantly "train" the algorithm to identify new developments or trends in hate speech or violent extremist speech on the internet.

In addition, an official for one company stated that algorithms are more effective at detecting potential violations for certain types of content than

---

[68]The official recalled one instance when the algorithm did not detect violative content and the violative content required manual removal.

other types of content. Specifically, the official stated that the company's algorithm is effective at reviewing text, images, and recorded audio, but faces more difficulty with reviewing live audio or video. As such, the company currently relies on users to report violative content that occurs on live audio or video to supplement the company's algorithm. Another company uses algorithms to automatically scan content such as virtual backgrounds, profile images, and files uploaded or exchanged through chat to detect and prevent violations of their policies.

According to officials from three companies, the potentially violative content flagged by users and the algorithm still needs to be reviewed by human moderators to understand the context in which it was posted. Officials from two companies told us the companies allow derogatory content to remain on their platforms after moderator review if the content is used in a re-appropriated context, such as for educational, documentary, scientific, or artistic purposes.

Research Suggests Up to One-Third of Internet Users Reported Experiencing Hate Speech on the Internet; Such Speech is Associated with Hate Crimes and Domestic Violent Extremist Incidents

Research studies we reviewed suggest that one-third of internet users experience hate speech on the internet, and that users post hate speech on the internet to spread hateful ideologies. In addition, research we reviewed, and DOJ and DHS reports suggest, that hate speech on the internet is associated with hate crimes and domestic violent extremist incidents.[69]

Some Research Shows that Up to One-Third of Internet Users Experience Hate Speech Online, but Exposure Differs based on Users' Characteristics

Four studies we reviewed showed that up to about a third of internet users who were surveyed reported experiencing hate speech on the internet.

- Three reports that provided findings from annual surveys of users' experiences on social media platforms found that the percentage of respondents who reported experiencing hate speech or harassment on the internet remained about the same, between 31 and 35 percent, from 2019 through 2022.[70]

- Another study surveyed users of internet gaming platforms and found that nearly 10 percent of players reported experiencing white supremacist speech in 2020 and 2021. Additionally, 50 percent of users in 2019 and 58 percent of users in 2021 reported experiencing

---

[69]For more detailed information on the scope and methodology of the literature review, see Appendix I.

[70]Anti-Defamation League, *Online Hate and Harassment: The American Experience 2020*, (New York, New York: 2020); Anti-Defamation League, *Online Hate and Harassment: The American Experience 2021*, (New York, New York: 2021); and Anti-Defamation League, *Online Hate and Harassment: The American Experience 2022*, (New York, New York: 2022).

discrimination from other players, due to age, gender, ethnicity, sexual orientation, or other characteristics.[71]

Four additional studies provided information on the characteristics of users who reported experiencing hate speech or hateful content on the internet.

- A 2019 study found that internet users with lower levels of income compared to those with medium and high levels of income reported more exposure to hate speech on the internet. In addition, the study found that male internet users reported more exposure to hate compared to female internet users.[72]

- A 2017 study found that women survey respondents reported experiencing more gender-based harassment in comparison to men (11 percent for women compared to 5 percent for men). This study also found that Black Americans (25 percent) and Hispanic Americans (10 percent) experienced more race-based harassment than White Americans (3 percent).[73]

- Another study analyzed reports of hate and harassment incidents against Asian Americans and Pacific Islanders between 2020 and 2021 and found that 10.1 percent of reports described discrimination on the internet.[74]

- A fourth study analyzed anti-Hindu content on select internet-based platforms and found that anti-Hindu content generally increased on these platforms from 2016 through 2022.[75]

Three of the studies in our review found that users who view hate speech on the internet experience negative mental health outcomes.

---

[71]Anti-Defamation League, *Hate is No Game: Harassment and Positive Social Experiences in Online Games 2021*, (New York, New York: 2021).

[72]Serkan Celik, "Experiences of Users Regarding Cyberhate," *Information Technology and People*, 2019, Vol. 32 No. 6, pp. 1446-1471.

[73]Maeve Duggan, *Online Harassment 2017*, (Washington, D.C.: Pew Research Center, 2017).

[74]Russel Jeung, Ronae Matriano, and Aggie Yellow Horse, *Stop AAPI Hate National Report*, (San Francisco, California: Stop AAPI Hate, 2021).

[75]John Farmer, Joel Finkelstein, Lee Jussim, Parth Parihar, Denver Riggleman, and Prasiddha Sudhakar, *Quantitative Methods for Investigating Anti-Hindu Disinformation*, (New Brunswick, New Jersey: Network Contagion Research Institute, 2022).

- One study found that viewing race-related violent and discriminatory content on social media may lead to negative social-emotional responses such as anxiety, sadness, anger, and fear.[76]

- A second study found that greater levels of social media usage and exposure to online racial discrimination during the COVID-19 pandemic were associated with anxiety, depression, and secondary traumatic stress.[77]

- Similarly, a third study found that a majority of respondents reported feeling angry, sad, or ashamed after exposure to hate speech on the internet, while over a third of respondents felt hateful, scared, or fearful.[78]

---

[76]Lauren Cestone, Nana Roest-Gyimah, Michelle Harris, Lani Jones, and Nelia Quezada, "Black Americans' Social Emotional Responses to Race-related Discriminatory Content on Social Media," *Journal of Ethnic and Cultural Diversity in Social Work*, October 2022. https://doi.org/10.1080/15313204.2022.2137716.

[77]Bo Feng, Samiksha Krishnamurthy, Alyan Layug, and Rachel McKenzie, "The Impacts of Social Media Use and Online Racial Discrimination on Asian American Mental Health: Cross-sectional Survey in the United States during COVID-19," *JMIR Formative Research*, 2022, Vol. 6 No. 9.

[78]Catherine Blaya, Matt Costello, James Hawdon, Vicente Llorent, Atte Oksanen, Pekka Räsänenm, Ashley Reichelmann, John Ryan, and Izabela Zych, "Hate Knows No Boundaries: Online Hate in Six Nations," *Deviant Behavior*, 2021, Vol. 42 No. 9, pp. 1100–1111.

Research Shows Users Post Hate Speech on the Internet to Spread and Reinforce Hateful Ideologies

> **Internet Used to Target Boston, Massachusetts Jewish Community, 2022**
>
> According to the Anti-Defamation League's "Audit of Antisemitic Incidents 2022" report, individuals or groups can use the internet to spread their message to a wider audience. As an example, the report mentioned the June 2022 Boston "Mapping Project" in which anti-Zionist activists published a website with the goal of "dismantling" organizations in Massachusetts that were "complicit" in Zionism. Approximately 500 entities were targeted, including many Jewish organizations that supported the local Jewish community. The "Mapping Project" provoked widespread fear in the Jewish community, and law enforcement, including the FBI, were put on high alert. After a U.S.-based website hosting company de-platformed the "Mapping Project," the website moved to an Iceland-based website hosting company.
>
> Source: Anti-Defamation League, *Audit of Antisemitic Incidents 2022*, (New York, New York: 2023).

According to three studies we reviewed, users who spread hate speech on the internet do so because the internet facilitates hate speech and helps reinforce hateful ideologies. Specifically, one research review found that the internet, and in particular social media platforms, is an effective tool for spreading propaganda and manipulation, allowing for the rapid spread of violence.[79] A second study found that users who were removed from some platforms for posting violative content had migrated to using other, niche, internet-based platforms. As a result, according to the study, these niche platforms were being used to cultivate U.S.-based hate speech and extremism for a range of radical ideologies.[80] Last, a third study found that one fifth of survey respondents in the U.S. reported feeling "proud" after they viewed hate speech on the internet, which the authors warned could be a dangerous indicator of increased white nationalism discourse in public.[81]

Four studies we reviewed examined how users who believed in certain violent extremist ideologies used the internet to spread hate speech.

- Two studies examined internet users who believed in misogynistic—hatred of or prejudice against women—violent extremism. One study found that posting inflammatory comments, pictures, or memes in public spaces on the internet allowed these individuals to construct or

---

[79]Neil Aggarwal, Laurence Kirmayer, and Cécile Rousseau, "Radicalization to Violence: A View from Cultural Psychiatry," *Transcultural Psychiatry*, 2021, Vol. 58(5), pp. 603–615.

[80]Andrew McCoy and Samantha Walther, "US Extremism on Telegram," *Perspectives on Terrorism*, April 2021, Vol. 15, No. 2, pp. 100-124.

[81]Blaya, Costello, Hawdon, Llorent, Oksanen, Räsänenm, Reichelmann, Ryan, and Zych, "Hate Knows No Boundaries: Online Hate in Six Nations."

adopt dominating masculine identities and perpetuate the idea of unequal gender relations.[82] The other study found that users who share similar moral worldviews online can develop deep connections within like-minded communities and were more likely to disseminate misogynistic rhetoric online.[83]

- Another study that conducted a content analysis of Ku Klux Klan-affiliated websites found that organizations and individuals associated with the Ku Klux Klan tended to use the internet to reinforce their teachings, deconstruct negative stereotypes about Klan members, and employ recruitment techniques framed around an ideology of social supremacy.[84]

- The fourth study analyzed hateful images—in the form of memes—associated with the "boogaloo" ideology and found that adherents used memes on the internet to spread information on how to plan for violence against religious and ethnic communities in the U.S.[85] The study also found that adherents of the boogaloo ideology incorporated "military language" into the hateful memes, appealing to an audience with military background.[86]

---

[82]Sarah Daly and Shon Reed, ""I Think Most of Society Hates Us": A Qualitative Thematic Analysis of Interviews with Incels," *Sex Roles,* 2022, Vol. 86, pp. 14–33.

[83]Mohammad Atari, Ian Anderson, Aida Mostafazadeh Davani, Morteza Dehghani, Brendan Kennedy, Drew Kogon, and Nripsuta Ani Saxena, "Morally Homogeneous Networks and Radicalism," *Social Psychological and Personality Science*, 2022, Vol. 13 No. 6, pp. 999-1009.

[84]Rachel Schmitz, "Intersections of Hate: Exploring the Transecting Dimensions of Race, Religion, Gender, and Family in Ku Klux Klan Web Sites," *Sociological Focus*, 2016, Vol. 49 No. 3, pp. 200-214.

[85]According 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. DOJ, U.S. Attorney's Office, Central District of California, *Pasadena Man Who Allegedly Adheres to Extremist Anti-Government Ideology Charged in Federal Complaint with Possessing Machine Gun*, Press Release (Los Angeles, California: January 26, 2023).

[86]Joel Finkelstein and Alex Goldenberg, *Cyber Swarming, Memetic Warfare and Viral Insurgency: How Domestic Militants Organize on Memes to Incite Violent Insurrection and Terror Against Government and Law Enforcement*, (New Brunswick, New Jersey: National Contagion Research Institute, 2020).

Research and Federal Agency Reports Suggest That Hate Speech on the Internet is Associated with Hate Crimes and Domestic Violent Extremist Incidents

Research Suggests an Association between Hate Speech on the Internet, Hate Crimes, and Bias-Motivated Domestic Violent Extremism

Five studies we reviewed suggested that an association exists between hate speech on the internet and the perpetration of hate crimes and bias-motivated domestic violent extremist incidents. In addition, three other studies generally found that people who consumed hate speech on the internet could be radicalized to participate in bias-motivated violent extremist acts.

- **Research suggests the occurrence of hate crimes is associated with hate speech on the internet.** Two studies found an association between hate speech on the internet and hate crimes by analyzing hate crime data at the local level. The first study found an association between uncivil comments toward Asians on the internet and the number of hate crimes against Asians in selected U.S. cities.[87] The second study found that counties with higher levels of internet access experienced higher levels of racially-motivated hate crimes on average.[88] According to the authors of the first study and based on additional findings from the second study, the association may be explained, at least in part, by varying levels of pre-existing racial discrimination in those localities.

  In addition, three other studies found that levels of hate speech on the internet and hate crimes appear to increase around key events in the U.S. For example, one of the studies found a spike in hate speech on an internet-based platform and in hate crimes in the same month as the Unite the Right rally in Charlottesville, Virginia in August 2017, where a violent extremist crashed his vehicle into a group of

---

[87]Bumsoo Kim, Eric Cooks, and Seong-Kyu Kim, "Exploring Incivility and Moral Foundations toward Asians in English-speaking Tweets in Hate Crime-reporting Cities during the COVID-19 Pandemic," *Internet Research*, January 2022, Vol. 32 No. 1, pp. 362-378.

[88]Jason Chan, Anindya Ghose, and Robert Seamans, "The Internet and Racial Hate Crime: Offline Spillovers from Online Access," *MIS Quarterly*, June 2016, Vol. 40 No. 2, pp. 381-403.

protestors, killing one of them.[89] The second study found spikes in hate speech on selected internet platforms around the time of the Charlottesville incident, and in the period leading up to the 2018 attack at the Tree of Life Synagogue in Pittsburgh, Pennsylvania.[90] A third study discussed earlier found that Black and Asian American gamers on the internet experienced increased levels of hate following the 2020 murder of George Floyd, and the 2021 spa shootings targeting Asians in Atlanta, Georgia.[91] These studies provide evidence of an association between hate speech and hate crimes or other violent extremist incidents, but do not imply causality. Increases in hate speech may occur in reaction to a hate crime or a violent incident.

- **Research suggests individuals radicalized on the internet can perpetrate violence as lone offenders.** For example, one study in our review that analyzed hate speech on the internet prior to a lone offender taking hostages at Congregation Beth Israel in Colleyville, Texas, found that the perpetrator's motive may have in part originated from content found on the internet.[92] A second study, discussed earlier, that found higher levels of racially-motivated hate crimes in counties with higher levels of internet access, reported that greater online access increased the frequency of hate crimes committed by lone offenders.[93] A third study analyzed a database of individuals radicalized in the U.S. who were either arrested, indicted, or killed as a result of perpetrating ideologically-motivated crimes, or were directly associated with a violent extremist organization. The study found that

[89]Brian Levin and Lisa Nakashima, *Report to the Nation: 2019, Factbook on Hate and Extremism in the U.S. and Internationally*, (San Bernardino, Calif.: California State University San Bernardino, 2019).

[90]Jason Baumgartner, Jack Donohue, John Farmer, Joel Finkelstein, Alex Goldenberg, Paul Goldenberg, Lee Jussim, Malav Modi, Pamela Paresky, Denver Riggleman, and Savvas Zannettou, *Antisemitic Disinformation: A Study of the Online Dissemination of Anti-Jewish Conspiracy Theories*, (New Brunswick, New Jersey: Network Contagion Research Institute, 2020).

[91]Anti-Defamation League, *Hate is No Game: Harassment and Positive Social Experiences in Online Games 2021.*

[92]Jack Donohue, Joel Finkelstein, Tayler Glover, Alex Goldenberg, Malav Modi, Heath Newton, Kiana Perst, Cristian Ramos, Denver Riggleman, and Prasiddha Sudhakar, *Sudden Massive Spike in Twitter Activity for "Free Aafia Movement" Preceded Attack on Congregation Beth Israel*, (New Brunswick, New Jersey: National Contagion Research Institute, 2021).

[93]Chan, Ghose, and Seamans, "The Internet and Racial Hate Crime: Offline Spillovers from Online Access."

while only 10.8 percent of violent extremists were radicalized on social media independently from an extremist group, these lone offenders had perpetrated deadlier bias-motivated attacks than those operating as group members.[94]

DHS and DOJ Have Reported That Hate Speech on the Internet Contributes to Hate Crimes and is Linked to Domestic Violent Extremist Incidents

DHS and DOJ have reported that hate speech on the internet played a role in some hate crimes and domestic violent extremist incidents. For instance, the U.S. Secret Service's National Threat Assessment Center reported that 42 out of 180 perpetrators of mass attacks in the U.S. from 2016 through 2020 (or about 23 percent) displayed concerning activity on the internet by threatening others and referencing suicidal thoughts, previous mass shootings, violent content, and hate toward people based on their actual or perceived characteristics.[95]

Further, three joint assessments issued by DHS and the FBI about domestic terrorism in the U.S. asserted that domestic violent extremists who plotted or carried out attacks were often radicalized to violence on the internet.[96] Specifically, the assessments stated that violent extremist content on the internet created opportunities for individuals to self-radicalize, connect with like-minded violent extremists, and conduct lone-offender or small-group attacks without the support of a larger violent extremist organization. In addition, based on our analysis of 120 domestic violent extremist incidents from 2016 through 2022 in DHS's Office of Intelligence and Analysis tracker, we identified at least 14 incidents (about 12 percent) that involved perpetrators who posted what we assessed as

---

[94]Mason Youngblood, "Extremist Ideology as a Complex Contagion: The Spread of Far-right Radicalization in the United States between 2005 and 2017," *Humanities and Social Sciences Communications*, 2020, Vol. 7:49.

[95]U.S. Secret Service National Threat Assessment Center, *Mass Attacks in Public Spaces: 2016-2020*, (Washington, D.C.: U.S. Department of Homeland Security, 2023).

[96]In FBI and DHS documentation the terms domestic terrorist and domestic violent extremist are used interchangeably. See: FBI and DHS, *Strategic Intelligence Assessment and Data on Domestic Terrorism* assessments published in May 2021, October 2022, and June 2023.

hate speech on the internet prior to carrying out a domestic terrorism incident.[97]

FBI and DHS have reviewed hate speech on the internet to help assess the risk for hate crimes and domestic violent extremist incidents, in certain circumstances.[98] For example, DHS's National Terrorism Advisory System Bulletin in effect from November 2022 to May 2023 cited examples of what we identified as hate speech on the internet as demonstrating an increased threat of violence against faith-based institutions, racial and religious minorities, and the LGBTQI+ community.[99] The following bulletin in effect from May 2023 to November 2023 continued to warn about calls for violence on the internet and that the likely targets of potential violence could be faith-based institutions, the LGBTQI+ community, and racial and religious minorities. Both bulletins also cited DHS's, FBI's, and the National Counterterrorism Center's issuance of the *U.S. Violent Extremist Mobilization Indicators* booklet that

---

[97]According to officials from DHS's Office of Intelligence and Analysis, the tracker of domestic violent extremist incidents does not track whether a domestic violent extremist incident involved hate speech on the internet. Rather, officials stated that information about the involvement of hate speech on the internet may be included in a summary about the incident. In addition, the tracker is updated on a quarterly basis to include information about new incidents or amend the information about previously identified incidents. We reviewed these summary statements to identify when DHS officials included information which we identified as hate speech on the internet in summaries associated with each incident.

[98]FBI's and DHS's review of hate speech on the internet is subject to investigative restrictions outlined in policy and informed by the constitution. For more information on FBI's and DHS's processes for investigating domestic terrorism or sharing information, including the use of open source information, see GAO, *Capitol Attack: Federal Agencies Identified Some Threats, but Did Not Fully Process and Share Information Prior to January 6, 2021*, GAO-23-106625 (Washington, D.C.: Feb. 28, 2023); GAO, *Domestic Terrorism: Further Actions Needed to Strengthen FBI and DHS Collaboration to Counter Threats*, GAO-23-104720 (Washington, D.C.: Feb. 22, 2023); and GAO, *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).

[99]While a number of variations on this acronym are currently in use to describe individuals with diverse sexual orientations and gender identities, in this report, we define LGBTQI+ as lesbian, gay, bisexual, transgender, queer, questioning, or intersex. The "plus" is meant to be inclusive of identities that may not be covered by the acronym LGBTQI, including asexual, non-binary, and individuals who identify their sexual orientation or gender identity in other ways.

provides guidance to help determine whether individuals are preparing to engage in violent extremist activities.[100]

The *U.S. Violent Extremist Mobilization Indicators* booklet provides information on how some of the observable behaviors may occur on the internet. Three indicators that may be observable on the internet are listed below along with publicly available information about federal prosecutions of hate crimes that we identified as illustrating a link between the crime and hate speech on the internet.

- **Communicating an intent to conduct violence.** Prior to an attack on a religious institution that resulted in physical damages, a perpetrator posted on social media that, "If we all kill just 1 [person of the religious minority] each tonight it will make a dent!"

- **Claiming religious, political, or ideological justification for a planned violent act.** A defendant pled guilty to hate crime charges following a mass shooting that killed and injured many people. Prior to the attack, the defendant posted to the internet how "the attack is a response to the [people of a certain national origin's] invasion of Texas. They are the instigators, not me. I am simply defending my country from cultural and ethnic replacement brought on by the invasion."

- **Implying an association with other violent extremists for the purpose of furthering violent activity.** A self-identified misogynistic ("involuntary celibate") violent extremist pled guilty to *attempting to commit a hate crime* by plotting to conduct a mass shooting of women. The defendant posted on the internet how bias-motivated actions he had undertaken (spraying women with juice from a water gun) were similar to the actions of another involuntary celibate violent extremist who perpetrated a previous attack and were "extremely empowering."

---

[100]The National Counterterrorism Center, within the Office of the Director of National Intelligence, conducts strategic operational planning for counterterrorism activities within and among agencies and serves as the primary organization for analyzing and integrating all intelligence pertaining to terrorism and counterterrorism, excepting intelligence pertaining exclusively to domestic terrorism and domestic counterterrorism. 50 U.S.C. § 3056(d). The agencies developed the indicators based on a review of FBI terrorism investigations, peer-reviewed academic studies, and analytic exchanges among Intelligence Community and law enforcement professionals. DHS. FBI, and National Counterterrorism Center, *U.S. Violent Extremist Mobilization Indicators*, 2021 Edition (Washington, D.C.: 2021).

Another violent extremism indicator of preparing for an attack involves issuing a threat. Depending on the severity and specificity of the threat, the threat could fall outside the parameters of constitutionally protected speech and thereby be considered a "true threat."[101] Thus, in some incidents, hate speech on the internet itself can become a criminal offense. For example, the FBI's UCR Program received 290 reports of hate crimes that occurred on the internet and involved the "intimidation" offense from 2016 through 2021.[102] In addition, based on our review of publicly available information from DOJ on federal prosecutions of bias-motivated crimes, the following are some examples of hate speech that were prosecuted as criminal offenses involving "true threats."[103]

- A defendant pled guilty to the charge of *interstate communication of threatening communications* after using a dictionary company's "Contact Us" webpage to send messages about committing violence against the company's employees. The defendant did so because the company included the concept of "gender identity" in its dictionary definition of different gender terms, such as "female" or "woman."

- A defendant pled guilty to the charge of *knowingly and intentionally transmitting a threatening communication in interstate commerce* after using a social media platform to send threatening messages to a victim based on the victim's race and national origin. The defendant

---

[101]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 and may constitute a criminal act. More specifically, such speech may be considered a hate crime if the necessary additional elements of the crime (e.g., bias motivation) are met. In some cases, federal prosecutors have also presented evidence of a perpetrator's off-line activity to demonstrate the seriousness of the threat, thus showing that the threat made on the internet was credible and "true." See *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). The most recent articulation of the true threat standard with respect to an online threatening communication was in *Counterman v. Colorado*, No. 22-138 (U.S. June 27, 2023). The Supreme Court held that to establish that a statement is a "true threat" unprotected by the First Amendment, the State must prove the defendant had some subjective understanding of their statements' threatening nature.

[102]According to FBI's *Hate Crime Data Collection Guidelines and Training Manual*, "intimidation" is defined as unlawfully placing another person in reasonable fear of harm through the use of threatening words and/or other conduct without displaying a weapon or subjecting the victim to an actual physical attack, including stalking.

[103]According to DOJ, additional statutes may be used to prosecute conduct involving true threats–including those which may involve bias motivation–beyond the hate crime statutes discussed previously. However, such statutes may not require DOJ to prove bias motivation as a necessary element of the crime and are therefore not characterized as "hate crime" statutes.

posted he would "rape and kill" the victim, and that he would "stop at nothing until you, your family, your friends, and the entire worthless…race is racially exterminated."

Conclusions

As company and research data show, substantial numbers of internet users have experienced hate on the internet in recent years. Additionally, our review of DOJ's press releases illustrates how some instances of hate speech on the internet were serious enough to constitute "true threats" against individual victims or groups, and were prosecuted by DOJ as criminal offenses. Although FBI's UCR Program collects data about hate crimes that occur on the internet from law enforcement agencies, BJS' National Crime Victimization Survey does not collect data from victims on bias-motivated victimization that occurs on the internet. While BJS' National Crime Victimization Survey could be a good source for collecting such information, BJS officials stated that they would need to do more research. However, BJS officials did not describe a plan to do so. Therefore, the National Crime Victimization Survey cannot complement similar data collected by the FBI related to hate crimes that occurred on the internet, which limits DOJ's ability to more readily produce a comprehensive understanding of national crime levels. Complementary data from FBI's UCR Program and BJS' National Crime Victimization Survey can jointly provide a more comprehensive understanding of national hate crime levels than either source could produce alone. For example, in 2019, law enforcement agencies reported 7,347 hate crimes to the FBI UCR Program, while BJS estimated that U.S. residents experienced approximately 305,390 bias-motivated victimizations based on the National Crime Victimization Survey. By exploring options to measure bias-motivated victimization that occurs on the internet in the National Crime Victimization Survey or in a supplemental survey, DOJ may be better positioned to understand crime trends and the nature of crime in the U.S. Collecting better data about victimization that occurs on the internet could also help DOJ identify communities that underreport hate incidents to law enforcement agencies and better inform resource allocation to communities affected by hate.

Recommendation for Executive Action

The Director of BJS should explore options to measure bias-motivated criminal victimization that occurs on the internet through the National Crime Victimization Survey or in a supplemental survey, as appropriate. (Recommendation 1)

Agency and Third Party Comments
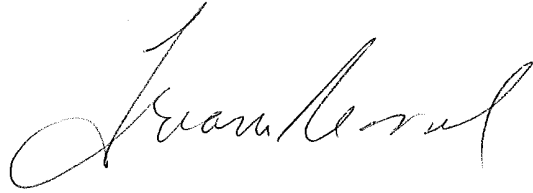
We provided a draft of this report to DHS and DOJ for review and comment. DHS did not provide written comments. DOJ provided formal, written comments, which are reproduced in full in appendix IV, and summarized below. Both DHS and DOJ provided technical comments, which we incorporated as appropriate. We also provided excerpts of the draft report for review and comment to the six companies operating internet-based platforms we contacted and whose data we present in this report, and incorporated technical comments from company officials as appropriate.

DOJ stated that BJS agreed with our recommendation that it explore options to measure bias-motivated criminal victimization that occurs on the internet through the National Crime Victimization Survey or in a supplemental survey, as appropriate. DOJ further noted that BJS will continue to conduct research on the intersection of crimes that are bias-motivated and occur on the internet, and based on that research, will determine how best to measure bias-motivated criminal victimization that occurs through the internet.

As agreed with your offices, 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, and the Secretary of Homeland Security. In addition, the report will be available at no charge on the GAO website at http://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 members who made key contributions to this report are listed in appendix V.

Triana McNeil
Director, Homeland Security and Justice

Appendix I: Objectives, Scope, and Methodology

This appendix provides additional information on our objectives, scope, and methodology. This report addresses the following: (1) the extent to which DOJ collects data on hate crimes that occur on the internet; (2) what company data indicate about steps selected companies have taken to remove hate speech and violent extremist speech from their internet platforms; and (3) what is known about users' experience with, or expression of, hate speech on the internet, and the relationship between hate speech on the internet and hate crimes and domestic violent extremism.

To address our first objective, we obtained and analyzed data from the FBI's Uniform Crime Reporting (UCR) Program on hate crimes that occurred on the internet between January 2016 and December 2021, the most recent data available during the time of this review.[1] This enabled us to describe the total number of reported hate crimes that occurred on the internet, as well as the types of offenses and bias motivations associated with hate crimes on the internet. To determine the reliability of these data, we reviewed FBI documentation about policies and procedures for law enforcement agencies to report hate crimes to the FBI's UCR Program, such as FBI's *Hate Crime Data Collection Guidelines and Training Manual*.[2] We also interviewed DOJ officials from FBI's Criminal Justice Information Services Division about the standards, policies, and procedures that the FBI's UCR Program uses to collect data on hate crimes that occur on the internet from federal, state, local, tribal, and

---

[1]Since the passage of the Hate Crime Statistics Act in 1990, the FBI has used its UCR Program to collect crime data from federal, state, local, tribal, and university law enforcement agencies. See 34 U.S.C. § 41305. The UCR Program generates statistics for use in law enforcement. It also provides information for students of criminal justice, researchers, the media, and the public. The UCR Program includes data from more than 18,000 city, university and college, county, state, tribal, and federal law enforcement agencies. In 2016, the UCR Program began collecting information on hate crimes that occur on the internet. We analyzed annual data on hate crime incidents that the FBI provided to us in July 2023 and reported incidents that met quality review standards provided by FBI officials. FBI officials told us that the full calendar year data for 2022 would not be available until fall 2023.

[2]FBI, Criminal Justice Information Services Division, *Hate Crime Data Collection Guidelines and Training Manual*, Version 3.0 (Washington, D.C.: March 1, 2022).

university law enforcement agencies.[3] Furthermore, we conducted
electronic data testing to identify outliers and ensure the completeness of
the data. We determined that the FBI's UCR data were reliable for the
purposes of describing the extent and characteristics of DOJ's collection
of data on hate crimes on the internet.

In addition, we interviewed DOJ officials from FBI's Criminal Justice
Information Services Division and DOJ's Office of Justice Programs about
support or technical assistance DOJ provides to law enforcement
agencies to improve the collection of FBI's UCR data on hate crimes. We
also interviewed six selected law enforcement agencies and one state
UCR Program about how they collect and report data on hate crimes that
occur on the internet to FBI's UCR Program. We selected agencies to
interview based on a variety of factors that included variation in
geographic dispersion, population size of the agency's jurisdiction,
agency type (such as city, county, university, state, or federal), and the
extent to which they reported hate crimes on the internet between 2016
and 2020.[4]

We also reviewed reports authored by or commissioned by DOJ's Bureau
of Justice Statistics (BJS) regarding the National Crime Victimization
Survey's collection of bias-motivated victimization data, such as
*Enhancing the Measurement of Hate Crime in the National Crime
Victimization Survey: Developing and Testing Improvements to the
Survey Questions*.[5] Additionally, we interviewed BJS officials regarding
procedures for the collection of such data and any steps the bureau was
taking to revise the survey to collect data on criminal victimization
committed on the internet. We reviewed BJS' plans for revising the survey
and compared them to requirements outlined in the Better Cybercrime
Metrics Act, *Standards for Internal Control in the Federal Government*

---

[3]For the purposes of this report, the term "local law enforcement agencies" refers to local,
tribal, and university law enforcement agencies collectively.

[4]At the time of selection, 2020 was the last complete year of UCR data on hate crimes
available from the FBI. The law enforcement agencies we interviewed were FBI's
Washington, D.C. Field Office; Lexington (Kentucky) Police Department; New Jersey
State Police Department; Skagit County (Washington) Sheriff's Office; University of
Michigan Police Department; Vermont State Police Department; and Worcester
(Massachusetts) Police Department.

[5]Sarah Cook, Chris Krebs, Yuli Patrick Hsieh, Lynn Langton, and Jerry Timbrook,
*Enhancing the Measurement of Hate Crime in the National Crime Victimization Survey:
Developing and Testing Improvements to the Survey Questions*, NCJ 301033 (Research
Triangle Park, North Carolina: RTI International, 2021).

related to using quality information, and the goals outlined in DOJ's Fiscal
Years 2022-2026 Strategic Plan.[6]

To address our second objective, we analyzed data and interviewed
officials from six selected companies that operate internet-based
platforms regarding their enforcement of policies on hate speech and
violent extremism.[7] To identify which companies to include in our review,
we examined 25 studies published between June 2016 and June 2022
from nongovernmental organizations about hate speech on the internet
and its relationship to hate crimes and domestic violent extremism.[8] We
also reviewed 94 news articles published between June 2019 and June
2022 describing hate crimes or domestic violent extremist incidents that
recently occurred. We counted how often studies and news articles cited
companies' internet-based platforms as where hate speech or violent
extremist speech occurred. We organized the companies by the number
of citations from most to least, and by the type of service the companies'
platforms provided, such as crowdfunding, livestreaming, or social media.

We reviewed whether the companies' publicly available policies explicitly
defined and prohibited platform users from using hate speech or violent
extremist speech. We then interviewed officials from the most cited
companies that had publicly available hate speech or violent extremist
speech policies, regarding how they enforce these policies and regarding
what data the companies track and publish about their enforcement of
these policies. Finally, we analyzed publicly available data, and data that
companies provided to us, to describe the amount of content and number
of users that violated the hate speech or violent extremist speech policies
from January 2018 through December 2022, for seven platforms operated
by six companies.[9] We analyzed enforcement data from companies in six-

---

[6]Pub. L. No. 117-116, 136 Stat. 1180 (2022); GAO, *Standards for Internal Control in the
Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014); U.S.
Department of Justice, *Fiscal Years 2022-2026 Strategic Plan,* (Washington, D.C.: 2022).

[7]Companies may use community guidelines, policies, and terms of service to define what
users are prohibited from doing—such as defining types of prohibited text, images, and
audio (i.e., violative content)—on the companies' platforms. For the purposes of this
report, we will refer to these collectively as policies.

[8]We selected this time frame to capture information to match the time frame used in the
first objective.

[9]Three of the companies operated four social media platforms. The other three companies
operated a livestreaming and media-hosting platform, a communication and messaging
platform, and a crowdfunding and financial transactions platform, respectively.

month time periods—January through June and July through
December—when complete data were available.

To address our third objective, we conducted a review of literature to
describe available research about (a) hate speech on the internet and (b)
its relationship to hate crimes and domestic violent extremism in the U.S.
published from January 2016 through October 2022.[10] To identify relevant
publications, we took the following steps:

1. We identified articles through an internet search for publicly available
   research and obtained additional recommendations from interviews
   with subject matter experts from a non-generalizable sample of
   nongovernmental organizations and think tanks.

2. A GAO research librarian also conducted a literature search of various
   research databases and platforms including ABI/Inform, EconLit,
   Homeland Security Digital Library, Scopus, and WorldCat, among
   others, to identify scholarly and peer-reviewed publications and
   publications by nonprofits and think tanks published from January
   2016 through October 2022.[11] We excluded conference proceedings,
   trade journal articles, law review articles, news articles, and
   summaries of congressional hearings and updates on bills as they
   move through congressional committees from the literature review.
   Our search terms and formulas included "internet," "social media,"
   "hate," "racism," "violen*," "crim*," "gender," and "sexual orientation,"
   among others. Two sets of abstract, title, and keyword searches were
   conducted to identify relevant articles.

3. To select the publications from steps 1 and 2 that were relevant to our
   research areas of (a) hate speech on the internet and (b) the
   relationship between hate speech on the internet and hate crimes and
   domestic violent extremism, two reviewers divided the set of
   publications and reviewed the abstracts for each publication, when

---

[10]We selected this time frame to match the same time frame used in the first and second
objectives.

[11]The full list of databases searched include: ABI/INFORM® Professional Advanced, APA
PsycInfo®, Computer and Information Systems Abstracts, Coronavirus Research
Database, Criminology Collection, EconLit, Education Database, Electronics &
Communications Abstracts, ERIC, Global Newsstream, Health & Medical Collection,
Homeland Security Digital Library, Index to Legal Periodicals (H.W. Wilson), Inspec®,
NTIS: National Technical Information Service, PAIS International, Policy File Index,
ProQuest Dissertations & Theses Global, PTSDpubs, Publicly Available Content
Database, Research Library, Risk Management Reference Center, SciSearch®: a Cited
Reference Science Database, SciTech Premium Collection, Scopus, Social SciSearch®,
Sociology Collection, Westlaw, and WorldCat.

available. If necessary, they reviewed the full text of the publication, to determine if it met the following criteria:

- If specified in the publication, a portion of the platform or internet users that were a focus of the publication must have been located in the U.S. If the location of users was not specifically stated in the article, then the team considered whether the platform studied was dedicated to a specific geographic area, and considered out of scope any articles focusing on platforms that specifically identified users in locations outside the U.S. If there was no mention of the location of the study, the team considered the study to be in scope, provided it met the other criterion, because internet users could have been located in the U.S.

- The type of online hate speech or extremist ideology is bias-motivated. Users must have expressed hate speech or violent extremist ideology on the internet consistent with the FBI's definition of hate crimes, which includes crimes committed on the basis of the victim's perceived or actual race, color, religion, national origin, sexual orientation, gender, gender identity, or disability.

4. To validate our scoping decisions, we selected a random sample of 10 percent of the articles that were determined to be out of scope, and these were verified by another analyst independently.

Out of a total 337 publications, 195 met the above two criteria and we reviewed the full text of the publication. We evaluated each publication using a data collection instrument that a team of GAO analysts filled out, working independently. The data collection instrument captured information on hate speech on the internet and the relationship between hate speech on the internet and hate crimes and domestic violent extremism identified in each publication in the following four categories, based on the scope of our review:

1. Information relevant to the demographic characteristics of users who post hate speech; the effect of this behavior on other users; or the format of hate speech posted online, such as videos, tweets, forum posts, manifestos, and social media posts.

2. Information identifying a specific time period or catalyzing event relevant to the online hate speech discussed in the study.

3. Information relevant to how internet users are motivated to post or participate in hate speech online or join groups or online spaces that facilitate this type of rhetoric.

4. Information relevant to the linkage, if any, between online hate speech
    and offline/real world attacks.[12]

If the article did not identify one of these themes, it was considered out of
scope for our review.

For each article determined to be in scope, a second reviewer then
reviewed the articles and made an independent determination. Any
differences in the reviewers' determinations about whether the article was
relevant and should be included in the review were discussed and
reconciled. The team identified 53 articles that contained relevant
information. The team then reviewed the relevant information within each
of the categories captured in the data collection instrument to identify key
themes among the literature that described findings related to hate
speech on the internet and the relationship between hate speech on the
internet and hate crimes and domestic violent extremism.

Further, for objective 3, we obtained and reviewed DOJ, FBI, and
Department of Homeland Security (DHS) reports about hate crimes,
including reports about criminal incidents we characterize as involving
bias-motivated domestic violent extremism. In addition, we interviewed
DOJ, FBI, and DHS officials, to describe when these federal agencies
have found evidence of a perpetrator's hate speech on the internet as
part of the agencies' investigations of hate crimes or violent extremist
incidents.[13] We also reviewed DOJ press releases regarding federal
prosecutions of hate crimes for 2016 through 2022, to describe instances
when DOJ indicated a perpetrator's hate speech on the internet was used
as evidence in prosecutions. Additionally, DHS provided us with
information on domestic terrorism incidents DHS collected and tracked
from 2016 through 2022.[14] We analyzed DHS's data to identify when an
incident included information that we assessed as hate speech posted to
the internet by a perpetrator prior to carrying out a domestic terrorism
incident.

---

[12]We also recorded any policy recommendations and discussions of the limitations of the
research relevant to one or more of the four themes.

[13]In this report, we refer to bias-motivated domestic violent extremism as violent
extremism ideologies in the territorial U.S. that are motivated by bias against protected
characteristics identified in federal hate crime statutes.

[14]We selected this time frame to capture information to match the time frame used in the
first objective.

We conducted this performance audit from November 2021 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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Types and Characteristics of Hate
Crimes that Occurred on the Internet Reported
to the Federal Bureau of Investigation (FBI)
from 2016 through 2021

Appendix II: Types and Characteristics of Hate Crimes that Occurred on the Internet Reported to the Federal Bureau of Investigation (FBI) from 2016 through 2021

From 2016 through 2021, federal, state, county, local, tribal, and university law enforcement agencies across the country reported 47,844 total hate crimes to the Federal Bureau of Investigation's (FBI) Uniform Crime Reporting (UCR) Program. Of the 47,844 total hate crimes reported to the FBI, 322 hate crimes occurred on the internet. The information below compares the most commonly reported categories for bias motivation, offense type, and offender race associated with hate crimes on the internet to the most commonly reported categories for the same variables associated with all other hate crimes reported by law enforcement agencies to FBI's UCR Program from 2016 through 2021.

The totals for each category may not always equal 100 percent due to rounding. Notably, the counts of each variable category may not equate to the total number of reported hate crimes during 2016 through 2021 because some hate crime reports that law enforcement agencies submit to the FBI may not include a value for each variable, or may include multiple values for a single variable. For example, some hate crime reports may describe hate crime incidents that involve more than one bias motivation, such as Anti-Black or African American and Anti-Gay (Male) recorded in one incident. In addition, some hate crime reports may not include an offender's race because the investigating law enforcement agency could not identify it. Our analysis counts each variable category associated with each incident in the data provided by the FBI.

Bias Motivation

In the Federal Bureau of Investigation's (FBI) Uniform Crime Reporting (UCR) Program, bias motivation is used to indicate whether an offense was motivated by the offender's bias and, if so, what type of bias. According to the data, 29 of the 34 possible bias motivations were associated with hate crimes that occurred on the internet. The most commonly reported bias motivation categories for hate crimes on the internet were generally consistent with the most commonly reported categories for all other hate crimes. However, for hate crimes on the internet, 5 percent of reported incidents were associated with an Anti-Gay (Male) bias motivation, compared to 10 percent for all other hate crimes.

Hate crimes on the internet
338 bias counts

- 41%
- 5% Anti-Gay (Male) (17)
- 9% Anti-White (31)
- 12% Anti-Jewish (42)
- 33% Anti-Black or African American (111)
- All other bias motivation categories (137)

All other hate crimes
48,605 bias counts

- 39%
- 10% Anti-Gay (Male) (4,654)
- 11% Anti-White (5,140)
- 11% Anti-Jewish (5,255)
- 30% Anti-Black or African American (14,475)
- All other bias motivation categories (19,081)

Offense

The UCR Program collects information on 81 offenses associated with hate crimes. According to the data, 11 of the 81 possible offense categories were associated with hate crimes that occurred on the internet. According to Department of Justice (DOJ) officials, some offenses such as simple assault or aggravated assault require a face-to-face interaction and cannot occur on the internet. According to the data, almost 90 percent of hate crimes on the internet involved intimidation, whereas 25 percent of all other hate crimes involved intimidation.

Hate crimes on the internet
325 offense counts

- 89%
- 5% All other offense categories (15)
- 2% False Pretenses/Swindle/Confidence Game (5)
- 2% Hacking/Computer Invasion (6)
- 3% Pornography/Obscene Material (9)
- Intimidation (290)

All other hate crimes
49,394 offense counts

- 13% Intimidation (12,532)
- All other offense categories (6,668)
- 12% Aggravated Assault (5,758)
- 22% Simple Assault (10,884)
- 27% Destruction/Damage/Vandalism of Property (13,552)
- 25%

Offender Race

The UCR Program also collects data on the race of offenders that commit hate crimes. According to the data, the most commonly reported offender race category associated with hate crimes that occurred on the internet was Unknown, followed by White, which is generally consistent with the top two most commonly reported offender race categories associated with all other hate crimes. However, for hate crimes on the internet, 8 percent of reported offenders were Black or African American, compared to 16 percent for all other hate crimes. The hate crime data we obtained from FBI's UCR Program includes only one data point on offender(s) race, even if the incident involved more than one offender. According to the 2021 National Incident-Based Reporting System User Manual, reporting agencies should submit an additional report to FBI's UCR Program if an investigation reveals the incident involved more than one offender.

Hate crimes on the internet
322 race counts

- 47%
- 3% All other offender race categories (10)
- 8% Black or African American (26)
- 42% White (136)
- Unknown (150)

All other hate crimes
47,522 race counts

- 41%
- 4% All other offender race categories (2,066)
- 16% Black or African American (7,486)
- 39% White (18,343)
- Unknown (19,627)

Source: GAO analysis of FBI's UCR Program data. | GAO-24-105553

Appendix II: Types and Characteristics of Hate
Crimes that Occurred on the Internet Reported
to the Federal Bureau of Investigation (FBI)
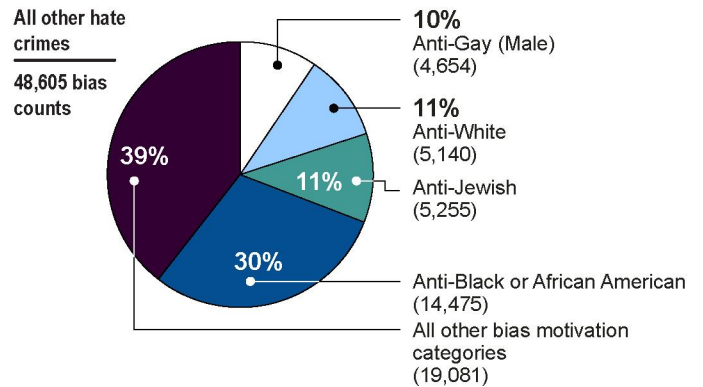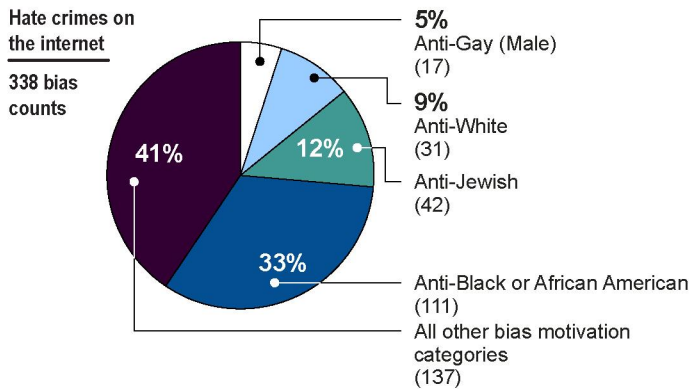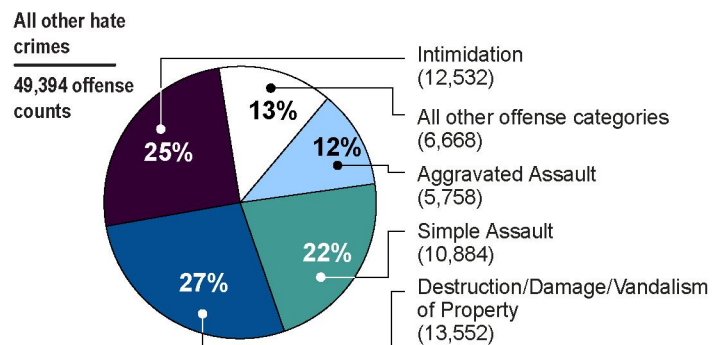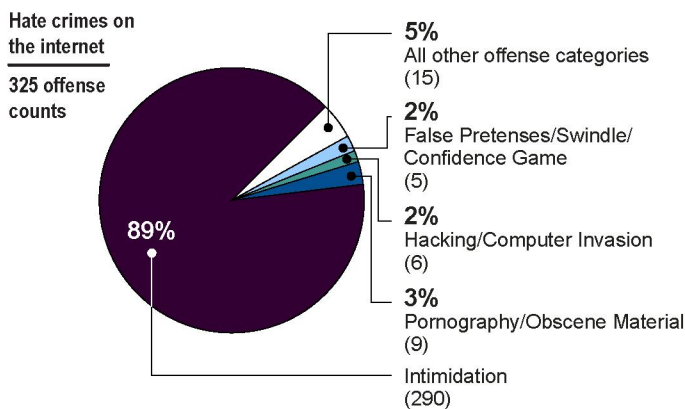from 2016 through 2021

Accessible Text and Data Tables for Bias Motivation, Offense, and Offender Race Graphic

Bias Motivation: In the Federal Bureau of Investigation's (FBI) Uniform Crime Reporting (UCR) Program, bias motivation is used to indicate whether an offense was motivated by the offender's bias and, if so, what type of bias. According to the data, 29 of the 34 possible bias motivations were associated with hate crimes that occurred on the internet. The most commonly reported bias motivation categories for hate crimes on the internet were generally consistent with the most commonly reported categories for all other hate crimes. However, for hate crimes on the internet, 5 percent of reported incidents were associated with an Anti-Gay (Male) bias motivation, compared to 10 percent for all other hate crimes.

Hate Crimes on the Internet	Bias Counts
All other bias motivation categories	137 (41%)
Anti-Black or African American	111 (33%)
Anti-Jewish	42 (12%)
Anti-White	31 (9%)
Anti-Gay (Male)	17 (5%)
Total	338 (100%)

All Other Hate Crimes	Bias Counts
All other bias motivation categories	19081 (39%)
Anti-Black or African American	14475 (30%)
Anti-Jewish	5255 (11%)
Anti-White	5140 (11%)
Anti-Gay (Male)	4654 (10%)
Total	48,605 (100%)

Offense: The UCR Program collects information on 81 offenses associated with hate crimes. According to the data, 11 of the 81 possible offense categories were associated wi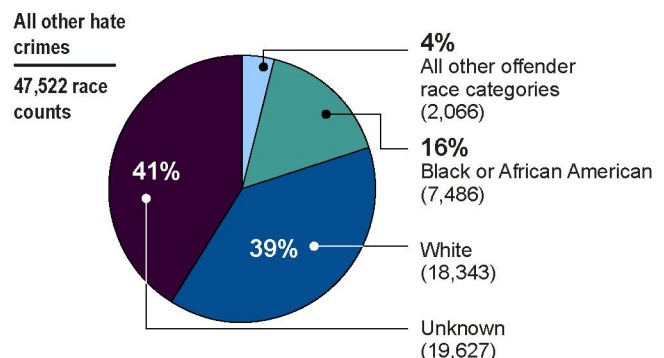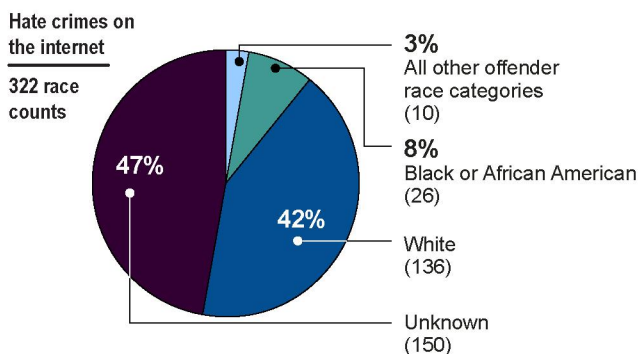th hate crimes that occurred on the internet. According to Department of Justice (DOJ) officials, some offenses such as simple assault or aggravated assault require a face-to-face interaction and cannot occur on the internet. According to the data, almost 90 percent of hate crimes on the internet involved intimidation, whereas 25 percent of all other hate crimes involved intimidation.

Hate Crimes on the Internet	Offense Counts
Intimidation	290 (89%)
Pornography/Obscene Material	9 (3%)
Hacking/Computer Invasion	6 (2%)
False Pretenses/Swindle/ Confidence Game	5 (2%)
All other offense categories	15 (5%)
Total	325 (100%)

All Other Hate Crimes	Offense Counts
Intimidation	12532 (25%)
Destruction/Damage/Vandalism of Property	13552 (27%)
Simple Assault	10884 (22%)
Aggravated Assault	5758 (12%)
All other offense categories	6668 (13%)
Total	49,394 (100%)

Appendix II: Types and Characteristics of Hate
Crimes that Occurred on the Internet Reported
to the Federal Bureau of Investigation (FBI)
from 2016 through 2021

Offender Race: The UCR Program also collects data on the race of offenders that commit hate crimes. According to the data, the most commonly reported offender race category associated with hate crimes that occurred on the internet was Unknown, followed by White, which is generally consistent with the top two most commonly reported offender race categories associated with all other hate crimes. However, for hate crimes on the internet, 8 percent of reported offenders were Black or African American, compared to 16 percent for all other hate crimes. The hate crime data we obtained from FBI's UCR Program includes only one data point on offender(s) race, even if the incident involved more than one offender. According to the 2021 National Incident- Based Reporting System User Manual, reporting agencies should submit an additional report to FBI's UCR Program if an investigation reveals the incident involved more than one offender.

Hate Crimes on the Internet	Race Counts
Unknown	150 (47%)
White	136 (42%)
Black or African American	26 (8%)
All other offender race categories	10 (3%)
Total	322 (100%)

All Other Hate Crimes	Race Counts
Unknown	19627 (41%)
White	18343 (39%)
Black or African American	7486 (16%)
All other offender race categories	2066 (4%)
Total	47,522 (100%)

Source: GAO analysis of FBI's UCR Program data. | GAO-24-105553

Appendix III: Number of Hate Crimes that
Occurred on the Internet Reported to the
Federal Bureau of Investigation (FBI), by State,
from 2016 through 2021

Appendix III: Number of Hate Crimes that Occurred on the Internet Reported to the Federal Bureau of Investigation (FBI), by State, from 2016 through 2021

Figure 8: Number of Hate Crimes that Occurred on the Internet Reported by Law Enforcement Agencies to the Federal Bureau of Investigation (FBI) by State between January 2016 and December 2021[a]

Source: GAO analysis of FBI's Uniform Crime Reporting Program data. | GAO-24-105553

Appendix III: Number of Hate Crimes that
Occurred on the Internet Reported to the
Federal Bureau of Investigation (FBI), by State,
from 2016 through 2021

Accessible Data Table for Figure 8: Number of Hate Crimes that Occurred on the Internet Reported by Law Enforcement Agencies to the Federal Bureau of Investigation (FBI) by State between January 2016 and December 2021[a]

	2016	2017	2018	2019	2020	2021
State	Cyberspace	Cyberspace	Cyberspace	Cyberspace	Cyberspace	Cyberspace
Alabama	0	0	0	0	0	0
Arizona	0	0	0	0	2	5
Arkansas	0	0	0	0	1	0
California	0	0	0	0	0	1
Colorado	0	0	0	2	4	2
Connecticut	0	0	2	0	2	5
Delaware	0	1	0	0	0	0
District of Columbia	0	0	0	0	0	0
Florida	0	0	0	0	0	0
Georgia	0	0	0	3	6	8
Idaho	0	0	0	0	2	0
Illinois	0	0	0	0	1	0
Indiana	0	0	0	1	2	4
Iowa	0	0	0	0	0	0
Kansas	0	0	0	0	0	0
Kentucky	0	2	3	0	1	2
Louisiana	0	0	0	0	0	2
Maine	0	0	0	0	0	0
Maryland	0	0	0	0	0	1
Massachusetts	0	1	2	1	3	2
Michigan	3	4	2	5	15	8
Minnesota	0	0	1	2	3	7
Mississippi	0	0	0	0	0	1
Missouri	0	0	1	3	0	0
Montana	0	0	0	0	0	0
Nebraska	0	0	0	0	0	1
Nevada	0	0	0	0	0	2
New Hampshire	0	0	0	0	1	0
New Jersey	0	0	0	0	0	31
New Mexico	0	0	0	0	0	0
New York	0	0	0	0	1	2
North Carolina	0	0	0	4	6	3
North Dakota	0	0	0	0	1	0
Ohio	0	0	0	1	1	1

Oklahoma	0	0	0	0	2	1
Oregon	0	1	0	1	0	1
Pennsylvania	0	0	0	0	0	1
Rhode Island	0	0	0	0	0	0
South Carolina	0	0	0	0	1	1
South Dakota	0	0	0	0	0	0
Tennessee	0	0	0	0	0	0
Texas	0	0	1	0	5	4
Utah	0	0	0	0	2	0
Vermont	0	0	0	0	2	0
Virginia	0	0	0	2	1	2
Washington	1	3	2	2	7	9
West Virginia	0	0	0	0	0	0
Wisconsin	0	1	1	1	5	5
Wyoming	0	0	0	0	0	0
Alaska	0	0	0	0	0	1
Hawaii	0	0	0	0	1	0

Source: GAO analysis of FBI's Uniform Crime Reporting Program data. | GAO-24-105553

[a]State, local, tribal, and university law enforcement agencies can voluntarily report hate crime data to the FBI's Uniform Crime Reporting Program. According to data we obtained from the FBI on the number of hate crimes that occurred on the internet between January 2016 and December 2021, law enforcement agencies in 12 states (Alabama, Florida, Iowa, Kansas, Maine, Montana, New Mexico, Rhode Island, South Dakota, Tennessee, West Virginia, and Wyoming) and the District of Columbia did not report any hate crimes that occurred on the internet during this time frame. This figure does not include data from U.S. territories.

Appendix IV: Comments from the Department of Justice

U.S. Department of Justice

Office of Justice Programs

Office of the Assistant Attorney General

Washington, D.C. 20531

December 15, 2023

Ms. Triana McNeil
Director
Homeland Security and Justice
Government Accountability Office
441 G Street, NW
Washington, DC 20548
VIA Electronic Mail at McNeilT@gao.gov

Dear Ms. McNeil:

Thank you for the opportunity to review and comment on the draft Government Accountability Office (GAO) report entitled, *Online Extremism: More Complete Information Needed About Hate Crimes that Occur on the Internet (GAO-24-105553).*

The draft GAO report contains one Recommendation for Executive Action directed to the Department of Justice, Office of Justice Programs (OJP). For ease of review, the recommendation directed to OJP is restated below and followed by our response.

1. **The Director of Bureau of Justice Statistics (BJS) should explore options to measure bias-motivated criminal victimization that occurs on the internet through the National Crime Victimization Survey or in a supplemental survey, as appropriate.**

   The Office of Justice Programs accepts this recommendation. The Bureau of Justice Statistics (BJS) currently measures bias-motivated criminal victimization through the National Crime Victimization Survey (NCVS). However, additional research is needed to identify, define, and measure behavior or conduct that occurs on the internet and determine whether this behavior or conduct meets the criteria of a bias-motivated crime under state and federal hate crime laws; specifically, whether this behavior or conduct demonstrates an attempted or actual commission of an act of harm.

   The NCVS is administered to persons aged 12 or older from a nationally representative sample of U.S. households. It collects information from respondents on nonfatal personal crimes (rape or sexual assault, robbery, aggravated assault, simple assault, and personal larceny (purse snatching and pocket picking) and household property crimes (burglary or trespassing, motor vehicle theft, and other types of theft). The survey collects information on threatened, attempted, and completed crimes. It collects both data and on crimes reported and not reported to police.

In September 2021, BJS issued a research report summarizing its review and assessment of state and federal hate crime laws, which was used to enhance the series of questions that are used in the NCVS to classify a victimization as a hate crime. The Hate Crime Statistics Act (34 U.S.C. § 41305) defines hate crimes as "crimes that manifest evidence of prejudice based on race, gender and gender identity, religion, disability, sexual orientation, or ethnicity." Additionally, through review of state laws, researchers identified three key elements that are present in state hate crime laws: (1) the offender's intent to cause harm to an individual, based on protected class characteristics; (2) identification of protected classes; and (3) the attempted or actual commission of an act of harm, through the offender's behavior or conduct.

Also, in response to the 2022 Better Cybercrime Metrics Act, BJS conducted research on cybercrime measurement, including: (1) existing cybercrime classifications/taxonomies, definitions, and measures (including state and federal laws and classifications from the International Classification of Crime for Statistical Purposes and the National Academies of Sciences, Engineering, and Medicine); (2) the existing measurement of cybercrime in the NCVS and a detailed comparison to the comprehensive cybercrime classification system by K. Phillips and colleagues (2022); and (3) recommendations for revision to the measurement of cybercrime in the NCVS.

BJS will continue to conduct research on the intersection of crimes that are bias-motivated and occur on the internet. Based on that research, BJS will determine how best to measure bias-motivated criminal victimization that occurs through the internet.

If you have any questions regarding this response, you or your staff may contact Jeffery Haley, Acting Director, Office of Audit, Assessment, and Management, at (202) 616-2936.

Sincerely,

Amy L. Solomon
Assistant Attorney General

cc: Thomas Jessor
        Assistant Director
        Homeland Security and Justice Team
        Government Accountability Office

        Jolene Ann Lauria
        Acting Assistant Attorney General for Administration
        U.S. Department of Justice

        Bradley Weinsheimer
        Associate Deputy Attorney General
        Office of the Deputy Attorney General

2

cc: Maureen A. Henneberg
           Deputy Assistant Attorney General

           Brent J. Cohen
           Acting Principal Deputy Assistant Attorney General

           Kevin M. Scott, Ph.D.
           Principal Deputy Director
           Bureau of Justice Statistics

           Rafael A. Madan
           General Counsel

           Jeffery Haley
           Acting Director
           Office of Audit, Assessment, and Management

           Rachel Johnson
           Chief Financial Officer
           Officer of the Chief Financial Officer

           Louise Duhamel
           Assistant Director, Audit Liaison Group
           Internal Review and Evaluation Office
           Justice Management Division

           OJP Executive Secretariat
           Correspondence Control Number: OCOM000651

3

Accessible Text for Appendix IV: Comments from the Department of Justice

December 15, 2023

Ms. Triana McNeil
Director
Homeland Security and Justice
Government Accountability Office
441 G Street, NW
Washington, DC 20548
VIA Electronic Mail at McNeilT@gao.gov

Dear Ms. McNeil:

Thank you for the opportunity to review and comment on the draft Government Accountability Office (GAO) report entitled, *Online Extremism: More Complete Information Needed About Hate Crimes that Occur on the Internet (GAO-24-105553).*

The draft GAO report contains one Recommendation for Executive Action directed to the Department of Justice, Office of Justice Programs (OJP). For ease of review, the recommendation directed to OJP is restated below and followed by our response.

The Director of Bureau of Justice Statistics (BJS) should explore options to measure bias-motivated criminal victimization that occurs on the internet through the National Crime Victimization Survey or in a supplemental survey, as appropriate.

The Office of Justice Programs accepts this recommendation. The Bureau of Justice Statistics (BJS) currently measures bias-motivated criminal victimization through the National Crime Victimization Survey (NCVS). However, additional research is needed to identify, define, and measure behavior or conduct that occurs on the internet and determine whether this behavior or conduct meets the criteria of a bias-motivated crime under state and federal hate crime laws; specifically, whether this behavior or conduct demonstrates an attempted or actual commission of an act of harm.

The NCVS is administered to persons aged 12 or older from a nationally representative sample of U.S. households. It collects information from respondents on nonfatal personal crimes (rape or sexual assault, robbery, aggravated assault, simple assault, and personal larceny (purse snatching and pocket picking) and

household property crimes (burglary or trespassing, motor vehicle theft, and other types of theft). The survey collects information on threatened, attempted, and completed crimes. It collects both data and on crimes reported and not reported to police.

In September 2021, BJS issued a research report summarizing its review and assessment of state and federal hate crime laws, which was used to enhance the series of questions that are used in the NCVS to classify a victimization as a hate crime. The Hate Crime Statistics Act (34 U.S.C. § 41305) defines hate crimes as "crimes that manifest evidence of prejudice based on race, gender and gender identity, religion, disability, sexual orientation, or ethnicity." Additionally, through review of state laws, researchers identified three key elements that are present in state hate crime laws: (1) the offender's intent to cause harm to an individual, based on protected class characteristics; (2) identification of protected classes; and (3) the attempted or actual commission of an act of harm, through the offender's behavior or conduct.

Also, in response to the 2022 Better Cybercrime Metrics Act, BJS conducted research on cybercrime measurement, including: (1) existing cybercrime classifications/taxonomies, definitions, and measures (including state and federal laws and classifications from the International Classification of Crime for Statistical Purposes and the National Academies of Sciences, Engineering, and Medicine); (2) the existing measurement of cybercrime in the NCVS and a detailed comparison to the comprehensive cybercrime classification system by K. Phillips and colleagues (2022); and (3) recommendations for revision to the measurement of cybercrime in the NCVS.

BJS will continue to conduct research on the intersection of crimes that are bias-motivated and occur on the internet. Based on that research, BJS will determine how best to measure bias-motivated criminal victimization that occurs through the internet.

If you have any questions regarding this response, you or your staff may contact Jeffery Haley, Acting Director, Office of Audit, Assessment, and Management, at (202) 616-2936.

Sincerely,

Amy L. Solomon   Assistant Attorney General

cc: Thomas Jessor
Assistant Director
Homeland Security and Justice Team
Government Accountability Office

Jolene Ann Lauria
Acting Assistant Attorney General for Administration
U.S. Department of Justice

Bradley Weinsheimer
Associate Deputy Attorney General
Office of the Deputy Attorney General

cc: Maureen A. Henneberg
Deputy Assistant Attorney General

Brent J. Cohen
Acting Principal Deputy Assistant Attorney General

Kevin M. Scott, Ph.D.
Principal Deputy Director
Bureau of Justice Statistics

Rafael A. Madan
General Counsel

Jeffery Haley
Acting Director
Office of Audit, Assessment, and Management

Rachel Johnson
Chief Financial Officer
Officer of the Chief Financial Officer

Louise Duhamel
Assistant Director, Audit Liaison Group
Internal Review and Evaluation Office
Justice Management Division

OJP Executive Secretariat
Correspondence Control Number: OCOM000651

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact named above, Tom Jessor (Assistant Director), Aaron Gluck (Analyst-in-Charge), Hiwotte Amare, Alex Aspiazu, Nasreen Badat, Benjamin Crossley, Susan Czachor, Christine Davis, Leia Dickerson, Susan Hsu, Amanda Miller, Jan Montgomery, Erin Pineda, Janet Temko-Blinder, Mary Turgeon, and Kellen Wartnow made key contributions to this report.

Related GAO Products

Violent Extremism: Agencies' and Financial Institutions' Efforts to Link Financing to Domestic Threats. GAO-23-105928. Washington, D.C.: September 13, 2023.

Homeland Security: Office of Intelligence and Analysis Should Improve Privacy Oversight and Assessment of Its Effectiveness. GAO-23-105475. Washington, D.C.: August 28, 2023.

Cybercrime: Reporting Mechanisms Vary, and Agencies Face Challenges in Developing Metrics. GAO-23-106080. Washington, D.C.: June 20, 2023.

Violent Extremism and Terrorism: Agencies Can Take Additional Steps to Counter Domestic Threats. GAO-23-106758. Washington, D.C.: June 15, 2023.

Capitol Attack: Federal Agencies Identified Some Threats, but Did Not Fully Process and Share Information Prior to January 6, 2021. GAO-23-106625. Washington, D.C.: February 28, 2023.

Domestic Terrorism: Further Actions Needed to Strengthen FBI and DHS Collaboration to Counter Threats. GAO-23-104720. Washington, D.C.: February 22, 2023.

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.

Capitol Attack: Additional Actions Needed to Better Prepare Capitol Police Officers for Violent Demonstrations. GAO-22-104829. Washington, D.C.: March 7, 2022.

Capitol Attack: The Capitol Police Need Clearer Emergency Procedures and a Comprehensive Security Risk Assessment. GAO-22-105001. Washington, D.C.: February 17, 2022.

Law Enforcement: DOJ Can Improve Publication of Use of Force Data and Oversight of Excessive Force Allegations. GAO-22-104456. Washington, D.C.: December 7, 2021.

K-12 Education: Students' Experiences with Bullying, Hate Speech, Hate Crimes, and Victimization in Schools. GAO-22-104341. Washington, D.C.: November 24, 2021.

Capitol Attack: Special Event Designations Could Have Been Requested for January 6, 2021, but Not All DHS Guidance is Clear. GAO-21-105255. Washington, D.C.: August 9, 2021.

Countering Violent Extremism: DHS Can Further Enhance Its Strategic Planning and Data Governance Efforts. GAO-21-507. Washington, D.C.: July 20, 2021.

Countering Violent Extremism: DHS Needs to Improve Grants Management and Data Collection. GAO-21-216. Washington, D.C.: February 1, 2021.

Religious-Based Hate Crimes: DOJ Needs to Improve Support to Colleges Given Increasing Reports on Campuses. GAO-20-6. Washington, D.C.: October 25, 2019.

Countering Violent Extremism: Actions Needed to Define Strategy and Assess Progress of Federal Efforts. GAO-17-300. Washington, D.C.: April 6, 2017.

Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate. GAO-11-605. Washington, D.C.: June 28, 2011.

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