theintercept.com

Leaked Documents Outline DHS's Plans to Police Disinformation

Ken Klippenstein, Lee Fang

31-40 minutes

The Department of Homeland Security is quietly broadening its efforts to curb speech it considers dangerous, an investigation by The Intercept has found. Years of internal DHS memos, emails, and documents — obtained via leaks and an ongoing lawsuit, as well as public documents — illustrate an expansive effort by the agency to influence tech platforms.

The work, much of which remains unknown to the American public, came into clearer view earlier this year when DHS announced a new "Disinformation Governance Board": a panel designed to police misinformation (false information spread unintentionally), disinformation (false information spread intentionally), and malinformation (factual information shared, typically out of context, with harmful intent) that allegedly threatens U.S. interests. While the board was widely ridiculed, immediately scaled back, and then shut down within a few months, other initiatives are underway as DHS pivots to monitoring social media now that its original mandate — the war on terror — has been wound down.

Behind closed doors, and through pressure on private platforms, the U.S. government has used its power to try to shape online discourse. According to meeting minutes and other records appended to a lawsuit filed by Missouri Attorney General Eric Schmitt, a Republican who is also running for Senate, discussions have ranged from the scale and scope of government intervention in online discourse to the mechanics of streamlining takedown requests for false or intentionally misleading information.

Key Takeaways

- Though DHS shuttered its controversial Disinformation Governance Board, a strategic document reveals the underlying work is ongoing.

- DHS plans to target inaccurate information on “the origins of the COVID-19 pandemic and the efficacy of COVID-19 vaccines, racial justice, U.S. withdrawal from Afghanistan, and the nature of U.S. support to Ukraine.”
- Facebook created a special portal for DHS and government partners to report disinformation directly.

  “Platforms have got to get comfortable with gov’t. It’s really interesting how hesitant they remain,” Microsoft executive Matt Masterson, a former DHS official, texted Jen Easterly, a DHS director, in February.

  In a March meeting, Laura Dehmlow, an FBI official, warned that the threat of subversive information on social media could undermine support for the U.S. government. Dehmlow, according to notes of the discussion attended by senior executives from Twitter and JPMorgan Chase, stressed that “we need a media infrastructure that is held accountable.”

“We do not coordinate with other entities when making content moderation decisions, and we independently evaluate content in line with the Twitter Rules,” a spokesperson for Twitter wrote in a statement to The Intercept.

There is also a formalized process for government officials to directly flag content on Facebook or Instagram and request that it be throttled or suppressed through a special Facebook portal that requires a government or law enforcement email to use. At the time of writing, the “content request system” at facebook.com/xtakedowns/login is still live. DHS and Meta, the parent company of Facebook, did not respond to a request for comment. The FBI declined to comment.

DHS’s mission to fight disinformation, stemming from concerns around Russian influence in the 2016 presidential election, began taking shape during the 2020 election and over efforts to shape discussions around vaccine policy during the coronavirus pandemic. Documents collected by The Intercept from a variety of sources, including current officials and publicly available reports, reveal the evolution of more active measures by DHS.

According to a draft copy of DHS’s Quadrennial Homeland Security Review, DHS’s capstone report outlining the department’s strategy and priorities in the coming years, the department plans to target

“inaccurate information” on a wide range of topics, including “the origins of the COVID-19 pandemic and the efficacy of COVID-19 vaccines, racial justice, U.S. withdrawal from Afghanistan, and the nature of U.S. support to Ukraine.”

“The challenge is particularly acute in marginalized communities,” the report states, “which are often the targets of false or misleading information, such as false information on voting procedures targeting people of color.”

The inclusion of the 2021 U.S. withdrawal from Afghanistan is particularly noteworthy, given that House Republicans, should they take the majority in the midterms, have vowed to investigate. “This makes Benghazi look like a much smaller issue,” said Rep. Mike Johnson, R-La., a member of the Armed Services Committee, adding that finding answers “will be a top priority.”

How disinformation is defined by the government has not been clearly articulated, and the inherently subjective nature of what constitutes disinformation provides a broad opening for DHS officials to make politically motivated determinations about what constitutes dangerous speech.

> The inherently subjective nature of what constitutes disinformation provides a broad opening for DHS officials to make politically motivated determinations about what constitutes dangerous speech.

DHS justifies these goals — which have expanded far beyond its original purview on foreign threats to encompass disinformation originating domestically — by claiming that terrorist threats can be “exacerbated by misinformation and disinformation spread online.” But the laudable goal of protecting Americans from danger has often been used to conceal political maneuvering. In 2004, for instance, DHS officials faced pressure from the George W. Bush administration to heighten the national threat level for terrorism, in a bid to influence voters prior to the election, according to former DHS Secretary Tom Ridge. U.S. officials have routinely lied about an array of issues, from the causes of its wars in Vietnam and Iraq to their more recent obfuscation around the role of the National Institutes of Health in funding the Wuhan Institute of Virology’s coronavirus research.

That track record has not prevented the U.S. government from

seeking to become arbiters of what constitutes false or dangerous information on inherently political topics. Earlier this year, Republican Gov. Ron DeSantis signed a law known by supporters as the “Stop WOKE Act,” which bans private employers from workplace trainings asserting an individual’s moral character is privileged or oppressed based on his or her race, color, sex, or national origin. The law, critics charged, amounted to a broad suppression of speech deemed offensive. The Foundation for Individual Rights and Expression, or FIRE, has since filed a lawsuit against DeSantis, alleging “unconstitutional censorship.” A federal judge temporarily blocked parts of the Stop WOKE Act, ruling that the law had violated workers’ First Amendment rights.

“Florida’s legislators may well find plaintiffs’ speech ‘repugnant.’ But under our constitutional scheme, the ‘remedy’ for repugnant speech is more speech, not enforced silence,” wrote Judge Mark Walker, in a colorful opinion castigating the law.

The extent to which the DHS initiatives affect Americans’ daily social feeds is unclear. During the 2020 election, the government flagged numerous posts as suspicious, many of which were then taken down, documents cited in the Missouri attorney general’s lawsuit disclosed. And a 2021 report by the Election Integrity Partnership at Stanford University found that of nearly 4,800 flagged items, technology platforms took action on 35 percent — either removing, labeling, or soft-blocking speech, meaning the users were only able to view content after bypassing a warning screen. The research was done “in consultation with CISA,” the Cybersecurity and Infrastructure Security Agency.

Prior to the 2020 election, tech companies including Twitter, Facebook, Reddit, Discord, Wikipedia, Microsoft, LinkedIn, and Verizon Media met on a monthly basis with the FBI, CISA, and other government representatives. According to NBC News, the meetings were part of an initiative, still ongoing, between the private sector and government to discuss how firms would handle misinformation during the election.

Homeland Security Secretary Kirstjen Nielsen stands alongside President Donald Trump as he speaks prior to signing the Cybersecurity and Infrastructure Security Agency Act in the Oval Office of the White House in Washington, D.C., on Nov. 16, 2018.

Photo: Saul Loeb/AFP via Getty Images

The stepped up counter-disinformation effort began in 2018 following high-profile hacking incidents of U.S. firms, when Congress passed and President Donald Trump signed the Cybersecurity and Infrastructure Security Agency Act, forming a new wing of DHS devoted to protecting critical national infrastructure. An August 2022 report by the DHS Office of Inspector General sketches the rapidly accelerating move toward policing disinformation.

From the outset, CISA boasted of an “evolved mission” to monitor social media discussions while “routing disinformation concerns” to private sector platforms.

In 2018, then-DHS Secretary Kirstjen Nielsen created the Countering Foreign Influence Task Force to respond to election disinformation. The task force, which included members of CISA as well as its Office of Intelligence and Analysis, generated “threat intelligence” about the election and notified social media platforms and law enforcement. At the same time, DHS began notifying social media companies about voting-related disinformation appearing on social platforms.

Key Takeaways, Cont'd.

- The work is primarily done by CISA, a DHS sub-agency tasked with protecting critical national infrastructure.
- DHS, the FBI, and several media entities are having biweekly meetings as recently as August.
- DHS considered countering disinformation relating to content that undermines trust in financial systems and courts.

- The FBI agent who primed social media platforms to take down the Hunter Biden laptop story continued to have a role in DHS policy discussions.

  In 2019, DHS created a separate entity called the Foreign Influence and Interference Branch to generate more detailed intelligence about disinformation, the inspector general report shows. That year, its staff grew to include 15 full- and part-time staff dedicated to disinformation analysis. In 2020, the disinformation focus expanded to include Covid-19, according to a Homeland Threat Assessment issued by Acting Secretary Chad Wolf.

  This apparatus had a dry run during the 2020 election, when CISA began working with other members of the U.S. intelligence community. Office of Intelligence and Analysis personnel attended "weekly teleconferences to coordinate Intelligence Community activities to counter election-related disinformation." According to the IG report, meetings have continued to take place every two weeks since the elections.

  Emails between DHS officials, Twitter, and the Center for Internet Security outline the process for such takedown requests during the period leading up to November 2020. Meeting notes show that the tech platforms would be called upon to "process reports and provide timely responses, to include the removal of reported misinformation from the platform where possible." In practice, this often meant state election officials sent examples of potential forms of disinformation to CISA, which would then forward them on to social media companies for a response.

  Under President Joe Biden, the shifting focus on disinformation has continued. In January 2021, CISA replaced the Countering Foreign Influence Task force with the "Misinformation, Disinformation and Malinformation" team, which was created "to promote more flexibility to focus on general MDM." By now, the scope of the effort had expanded beyond disinformation produced by foreign governments to include domestic versions. The MDM team, according to one CISA official quoted in the IG report, "counters all types of disinformation, to be responsive to current events."

  Jen Easterly, Biden's appointed director of CISA, swiftly made it clear that she would continue to shift resources in the agency to combat the spread of dangerous forms of information on social

media. “One could argue we’re in the business of critical infrastructure, and the most critical infrastructure is our cognitive infrastructure, so building that resilience to misinformation and disinformation, I think, is incredibly important,” said Easterly, speaking at a conference in November 2021.

CISA’s domain has gradually expanded to encompass more subjects it believes amount to critical infrastructure. Last year, The Intercept reported on the existence of a series of DHS field intelligence reports warning of attacks on cell towers, which it has tied to conspiracy theorists who believe 5G towers spread Covid-19. One intelligence report pointed out that these conspiracy theories “are inciting attacks against the communications infrastructure.”

CISA has defended its burgeoning social media monitoring authorities, stating that “once CISA notified a social media platform of disinformation, the social media platform could independently decide whether to remove or modify the post.” But, as documents revealed by the Missouri lawsuit show, CISA’s goal is to make platforms more responsive to their suggestions.

In late February, Easterly texted with Matthew Masterson, a representative at Microsoft who formerly worked at CISA, that she is “trying to get us in a place where Fed can work with platforms to better understand mis/dis trends so relevant agencies can try to prebunk/debunk as useful.”

Meeting records of the CISA Cybersecurity Advisory Committee, the main subcommittee that handles disinformation policy at CISA, show a constant effort to expand the scope of the agency’s tools to foil disinformation.

In June, the same DHS advisory committee of CISA — which includes Twitter head of legal policy, trust, and safety Vijaya Gadde and University of Washington professor Kate Starbird — drafted a report to the CISA director calling for an expansive role for the agency in shaping the “information ecosystem.” The report called on the agency to closely monitor “social media platforms of all sizes, mainstream media, cable news, hyper partisan media, talk radio and other online resources.” They argued that the agency needed to take steps to halt the “spread of false and misleading information,” with a focus on information that undermines “key

democratic institutions, such as the courts, or by other sectors such as the financial system, or public health measures."

To accomplish these broad goals, the report said, CISA should invest in external research to evaluate the "efficacy of interventions," specifically with research looking at how alleged disinformation can be countered and how quickly messages spread. Geoff Hale, the director of the Election Security Initiative at CISA, recommended the use of third-party information-sharing nonprofits as a "clearing house for trust information to avoid the appearance of government propaganda."

Last Thursday, immediately following billionaire Elon Musk's completed acquisition of Twitter, Gadde was terminated from the company.

Alejandro Mayorkas, secretary of the Department of Homeland Security, speaks during a new conference in Brownsville, Texas, on Aug. 12, 2021.

Photo: Veronica G. Cardenas/Bloomberg via Getty Images

The Biden administration, however, did take a stab at making part of this infrastructure public in April 2022, with the announcement of the Disinformation Governance Board. The exact functions of the board, and how it would accomplish its goal of defining and combating MDM, were never made clear.

The board faced immediate backlash across the political spectrum. "Who among us thinks the government should add to its work list the job of determining what is true and what is disinformation? And who thinks the government is capable of telling the truth?" wrote Politico media critic Jack Shafer. "Our government produces lies

and disinformation at industrial scale and always has. It overclassifies vital information to block its own citizens from becoming any the wiser. It pays thousands of press aides to play hide the salami with facts."

DHS Secretary Alejandro Mayorkas alluded to broad scope of the agency's disinformation effort when he told the Senate Homeland Security and Governmental Affairs Committee that the role of the board — which by that point had been downgraded to a "working group" — is to "actually develop guidelines, standards, guardrails to ensure that the work that has been ongoing for nearly 10 years does not infringe on people's free speech rights, rights of privacy, civil rights, and civil liberties."

"It was quite disconcerting, frankly," he added, "that the disinformation work that was well underway for many years across different independent administrations was not guided by guardrails."

DHS eventually scrapped the Disinformation Governance Board in August. While free speech advocates cheered the dissolution of the board, other government efforts to root out disinformation have not only continued but expanded to encompass additional DHS sub-agencies like Customs and Border Protection, which "determines whether information about the component spread through social media platforms like Facebook and Twitter is accurate." Other agencies such as Immigration and Customs Enforcement, the Science and Technology Directorate (whose responsibilities include "determining whether social media accounts were bots or humans and how the mayhem caused by bots affects behavior"), and the Secret Service have also expanded their purview to include disinformation, according to the inspector general report.

The draft copy of DHS's 2022 Quadrennial Homeland Security Review reviewed by The Intercept also confirms that DHS views the issue of tackling disinformation and misinformation as a growing portion of its core duties. While "counterterrorism remains the first and most important mission of the Department," it notes, the agency's "work on these missions is evolving and dynamic" and must now adapt to terror threats "exacerbated by misinformation and disinformation spread online" including by "domestic violent extremists."

To accomplish this, the draft quadrennial review calls for DHS to "leverage advanced data analytics technology and hire and train skilled specialists to better understand how threat actors use online platforms to introduce and spread toxic narratives intended to inspire or incite violence, as well as work with NGOs and other parts of civil society to build resilience to the impacts of false information."

The broad definition of "threat actors" posing risks to vaguely defined critical infrastructure — an area as broad as trust in government, public health, elections, and financial markets — has concerned civil libertarians. "No matter your political allegiances, all of us have good reason to be concerned about government efforts to pressure private social media platforms into reaching the government's preferred decisions about what content we can see online," said Adam Goldstein, the vice president of research at FIRE.

"Any governmental requests to social media platforms to review or remove certain content," he added, "should be made with extreme transparency."

A tweet about the FBI is displayed during a Senate Homeland Security and Governmental Affairs Committee hearing regarding social media's impact on homeland security on Capitol Hill in Washington, D.C., on Sept. 14, 2022.

Photo: Stefani Reynolds/AFP via Getty Images

DHS's expansion into misinformation, disinformation, and malinformation represents an important strategic retooling for the

agency, which was founded in 2002 in response to the 9/11 attacks as a bulwark to coordinate intelligence and security operations across the government. At the same time, the FBI deployed thousands of agents to focus on counterterrorism efforts, through building informant networks and intelligence operations designed to prevent similar attacks.

But traditional forms of terrorism, posed by groups like Al Qaeda, evolved with the rise of social media, with groups like the Islamic State using platforms such as Facebook to recruit and radicalize new members. After initial reluctance, social media giants worked closely with the FBI and DHS to help monitor and remove ISIS-affiliated accounts.

FBI Director James Comey told the Senate Intelligence Committee that law enforcement agencies needed to rapidly "adapt and confront the challenges" posed by terror networks that had proven adept at tapping into social media. Intelligence agencies backed new startups designed to monitor the vast flow of information across social networks to better understand emerging narratives and risks.

"The Department has not been fully reauthorized since its inception over fifteen years ago," the Senate Homeland Security Committee warned in 2018. "As the threat landscape continues to evolve, the Department adjusted its organization and activities to address emerging threats and protect the U.S. homeland. This evolution of the Department's duties and organization, including the structure and operations of the DHS Headquarters, has never been codified in statute."

The subsequent military defeat of ISIS forces in Syria and Iraq, along with the withdrawal from Afghanistan, left the homeland security apparatus without a target. Meanwhile, a new threat entered the discourse. The allegation that Russian agents had seeded disinformation on Facebook that tipped the 2016 election toward Donald Trump resulted in the FBI forming the Foreign Influence Task Force, a team devoted to preventing foreign meddling in American elections.

According to DHS meeting minutes from March, the FBI's Foreign Influence Task Force this year includes 80 individuals focused on curbing "subversive data utilized to drive a wedge between the

populace and the government."

"The Department will spearhead initiatives to raise awareness of disinformation campaigns targeting communities in the United States, providing citizens the tools necessary to identify and halt the spread of information operations intended to promote radicalization to violent extremism or mobilization to violence," DHS Acting Secretary Kevin McAleenan said in a September 2019 strategic framework.

DHS also began to broaden its watch to include a wide array of domestic actors viewed as potential sources of radicalization and upheaval. An FBI official interviewed by The Intercept described how, in the summer of 2020, amid the George Floyd protests, he was reassigned from his normal job of countering foreign intelligence services to monitoring American social media accounts. (The official, not authorized to speak publicly, described the reassignment on condition of anonymity.)

And a June 2020 memo bearing the subject line "Actions to Address the Threat Posed by Domestic Terrorists and Other Domestic Extremists" prepared by DHS headquarters for Wolf, Trump's acting DHS secretary, delineates plans to "expand information sharing with the tech sector" in order to "identify disinformation campaigns used by DT [domestic terrorism] actors to incite violence against infrastructure, ethnic, racial or religious groups, or individuals." The memo outlines plans to work with private tech sector partners to share unclassified DHS intelligence on "DT actors and their tactics" so that platforms can "move effectively use their own tools to enforce user agreements/terms of service and remove DT content."

Biden also prioritized such efforts. Last year, the Biden administration released the first National Strategy for Countering Domestic Terrorism. The strategy identified a "broader priority: enhancing faith in government and addressing the extreme polarization, fueled by a crisis of disinformation and misinformation often channeled through social media platforms, which can tear Americans apart and lead some to violence."

"We are working with like-minded governments, civil society, and the technology sector to address terrorist and violent extremist content online, including through innovative research

collaborations," the strategy document continued, adding that the administration was "addressing the crisis of disinformation and misinformation, often channeled through social and other media platforms, that can fuel extreme polarization and lead some individuals to violence."

Last year, a top FBI counterterrorism official came under fire when she falsely denied to Congress that the FBI monitors Americans' social media and had therefore missed threats leading up to the attack on the U.S. Capitol on January 6, 2021. In fact, the FBI has spent millions of dollars on social media tracking software like Babel X and Dataminr. According to the bureau's official guidelines, authorized activities include "proactively surfing the Internet to find publicly accessible websites and services through which recruitment by terrorist organizations and promotion of terrorist crimes is openly taking place."

Another FBI official, a joint terrorism task force officer, described to The Intercept being reassigned this year from the bureau's international terrorism division, where they had primarily worked on cases involving Al Qaeda and the Islamic State group, to the domestic terrorism division to investigate Americans, including anti-government individuals such as racially motivated violent extremists, sovereign citizens, militias, and anarchists. They work on an undercover basis online to penetrate social networking chat rooms, online forums, and blogs to detect, enter, dismantle, and disrupt existing and emerging terrorist organizations via online forums, chat rooms, bulletin boards, blogs, websites, and social networking, said the FBI official, who did not have permission to speak on the record.

The Privacy Act of 1974, enacted following the Watergate scandal, restricts government data collection of Americans exercising their First Amendment rights, a safeguard that civil liberty groups have argued limits the ability of DHS and the FBI to engage in surveillance of American political speech expressed on social media. The statute, however, maintains exemptions for information collected for the purposes of a criminal or law enforcement investigation.

"There are no specific legal constraints on the FBI's use of social media," Faiza Patel, senior director of the Brennan Center for

Justice's liberty and national security program told The Intercept. "The attorney general guidelines permit agents to look at social media before there is any investigation at all. So it's kind of a Wild West out there."

The first FBI official, whom The Intercept interviewed in 2020 amid the George Floyd riots, lamented the drift toward warrantless monitoring of Americans saying, "Man, I don't even know what's legal anymore."

In retrospect, the New York Post reporting on the contents of Hunter Biden's laptop ahead of the 2020 election provides an elucidating case study of how this works in an increasingly partisan environment.

Much of the public ignored the reporting or assumed it was false, as over 50 former intelligence officials charged that the laptop story was a creation of a "Russian disinformation" campaign. The mainstream media was primed by allegations of election interference in 2016 — and, to be sure, Trump did attempt to use the laptop to disrupt the Biden campaign. Twitter ended up banning links to the New York Post's report on the contents of the laptop during the crucial weeks leading up to the election. Facebook also throttled users' ability to view the story.

In recent months, a clearer picture of the government's influence has emerged.

In an appearance on Joe Rogan's podcast in August, Meta CEO Mark Zuckerberg revealed that Facebook had limited sharing of the New York Post's reporting after a conversation with the FBI. "The background here is that the FBI came to us — some folks on our team — and was like, 'Hey, just so you know, you should be on high alert that there was a lot of Russian propaganda in the 2016 election,'" Zuckerberg told Rogan. The FBI told them, Zuckerberg said, that "'We have it on notice that basically there's about to be some kind of dump.'" When the Post's story came out in October 2020, Facebook thought it "fit that pattern" the FBI had told them to look out for.

Zuckerberg said he regretted the decision, as did Jack Dorsey, the CEO of Twitter at the time. Despite claims that the laptop's contents were forged, the Washington Post confirmed that at least some of the emails on the laptop were authentic. The New York Times

authenticated emails from the laptop — many of which were cited in the original New York Post reporting from October 2020 — that prosecutors have examined as part of the Justice Department's probe into whether the president's son violated the law on a range of issues, including money laundering, tax-related offenses, and foreign lobbying registration.

Documents filed in federal court as part of a lawsuit by the attorneys general of Missouri and Louisiana add a layer of new detail to Zuckerberg's anecdote, revealing that officials leading the push to expand the government's reach into disinformation also played a quiet role in shaping the decisions of social media giants around the New York Post story.

According to records filed in federal court, two previously unnamed FBI agents — Elvis Chan, an FBI special agent in the San Francisco field office, and Dehmlow, the section chief of the FBI's Foreign Influence Task Force — were involved in high-level communications that allegedly "led to Facebook's suppression" of the Post's reporting.

The Hunter Biden laptop story was only the most high-profile example of law enforcement agencies pressuring technology firms. In many cases, the Facebook and Twitter accounts flagged by DHS or its partners as dangerous forms of disinformation or potential foreign influence were clearly parody accounts or accounts with virtually no followers or influence.

In May, Missouri Attorney General Eric Schmitt took the lead in filing a lawsuit to combat what he views as sweeping efforts by the Biden administration to pressure social media companies to moderate certain forms of content appearing on their platforms.

The suit alleges governmentwide efforts to censor certain stories, especially ones related to the pandemic. It also names multiple agencies across the government that have participated in efforts to monitor speech and "open collusion" between the administration and social media companies. It identifies, for example, emails between officials from the National Institutes of Health, including Dr. Anthony Fauci, and Zuckerberg at the beginning of the pandemic, and reveals ongoing discussions between senior Biden administration officials with Meta executives on developing content moderation policies on a range of issues, including issues related to

elections and vaccines.

Attorneys for the Biden administration have responded in court by claiming that the plaintiffs lack standing and that social media firms pursued content moderation policies on their own volition, without any "coercive" influence from the government. On October 21, the judge presiding over the case granted the attorneys general permission to depose Fauci, CISA officials, and communication specialists from the White House.

While the lawsuit has a definite partisan slant, pointing the finger at the Biden administration for allegedly seeking to control private speech, many of the subpoenas request information that spans into the Trump era and provides a window into the absurdity of the ongoing effort.

"There is growing evidence that the legislative and executive branch officials are using social media companies to engage in censorship by surrogate," said Jonathan Turley, a professor of law at George Washington University, who has written about the lawsuit. "It is axiomatic that the government cannot do indirectly what it is prohibited from doing directly. If government officials are directing or facilitating such censorship, it raises serious First Amendment questions."

During the 2020 election, the Department of Homeland Security, in an email to an official at Twitter, forwarded information about a potential threat to critical U.S. infrastructure, citing FBI warnings, in this case about an account that could imperil election system integrity.

The Twitter user in question had 56 followers, along with a bio that read "dm us your weed store locations (hoes be mad, but this is a parody account)," under a banner image of Blucifer, the 32-foot-tall demonic horse sculpture featured at the entrance of the Denver International Airport.

"We are not sure if there's any action that can be taken, but we wanted to flag them for consideration," wrote a state official on the email thread, forwarding on other examples of accounts that could be confused with official government entities. The Twitter representative responded: "We will escalate. Thank you."

Each email in the chain carried a disclaimer that the agency "neither has nor seeks the ability to remove or edit what information

is made available on social media platforms."

That tagline, however, concerns free speech advocates, who note that the agency is attempting to make an end run around the First Amendment by exerting continual pressure on private sector social media firms. "When the government suggests things, it's not too hard to pull off the velvet glove, and you get the mail fist," said Adam Candeub, a professor of law at Michigan State University. "And I would consider such actions, especially when it's bureaucratized, as essentially state action and government collusion with the platforms."

"If a foreign authoritarian government sent these messages," noted Nadine Strossen, the former president of the American Civil Liberties Union, "there is no doubt we would call it censorship."