MERCOLA
Take Control of Your Health

How Many Secrets Is the President Hiding?

Analysis by Dr. Joseph Mercola | December 12, 2023

STORY AT-A-GLANCE

- Over the past year, the House Judiciary Subcommittee on the Weaponization of the Federal Government has released several reports detailing how the government is a) harassing and intimidating citizens to shut down undesirable viewpoints b) using misinformation and propaganda to drive false narratives and c) censoring protected speech using third parties
- November 30, 2023, House Judiciary Committee held another hearing on the Weaponization of the Federal Government. Investigative journalist Michael Shellenberger testified and shared evidence about the existence of a group called the Cyber Threat Intelligence League (CTIL), which consists of military contractors that are censoring Americans and using sophisticated psychological operations against us
- The CTIL was founded by a group of former Israeli and British intelligence agents who initially volunteered their cybersecurity services FOR FREE to multibillion-dollar hospital and health care organizations in the U.S.
- CTIL also offers physical security and "cognitive" security, which are volunteered by U.S. and British military contractors
- The CTIL's plan to control the information landscape also includes using debanking as financial leverage, pressuring social media platforms to change their terms of service to facilitate censorship and deplatforming under the guise of "terms of service violations," and more

The video above features the November 30, 2023, House Judiciary Committee hearing on the Weaponization of the Federal Government.[1]

Over the past year, the Subcommittee on the Weaponization of the Federal Government has released several reports detailing how the government is a) harassing and intimidating citizens to shut down undesirable viewpoints, b) using misinformation and propaganda to drive false narratives and c) censoring protected speech using third parties. Here's a list of those reports that you can peruse at your convenience.

- "The Weaponization of the Federal Trade Commission: An Agency's Overreach to Harass Elon Musk's Twitter," March 7, 2023
- Interim Report on AG Garland's Anti-Parent Memo, March 21, 2021
- "The Hunter Biden Statement: How Senior Senior Intelligence Community Officials and the Biden Campaign Worked to Mislead American Voters," May 10, 2023
- "Report on FBI Whistleblower Testimony Highlights Government Abuse, Misallocation of Resources, and Retaliation," May 18, 2023
- "The Weaponization of CISA: How a 'Cybersecurity' Agency Colluded with Big Tech and 'Disinformation' Partners to Censor Americans," June 26, 2023
- "The FBI's Collaboration with a Compromised Ukrainian Intelligence Agency to Censor American Speech," July 10, 2023
- "Fighting the Weaponization of the Internal Revenue Service (IRS): The End of Abusive Unannounced Field Visits," October 27, 2023
- "The Weaponization of 'Disinformation' Pseudo-experts and Bureaucrats: How the Federal Government Partnered with Universities to Censor Americans' Free Speech," November 6, 2023
- Jira Ticket Data, which prove government was mass censoring vaccine information
- "The FBI's Breach of Religious Freedom: The Weaponization of Law Enforcement Against Catholic Americans," December 4, 2023

"The Justice Department's Deviations from Standard Processes in its Investigation of Hunter Biden," December 5, 2023

The Subcommittee also filed an amicus brief on Missouri v. Biden in early August 2023.

Rep. Thomas Massie Censored

Around the one-hour mark in the featured video, Rep. Thomas Massie questions Olivia Troye — a former intelligence official at the Department of Homeland Security under President Obama and a national security and counterterrorism adviser to vice president Mike Pence — about the U.S. government's use of third party organizations to censor protected speech.

The relevant clip is included above. In her opening statement, Troye accused the Committee of "indulging in fantasy detached from reality." "Members of this committee and their witnesses make grand and vague accusations about government censorship," she said. She also claimed the members were "spreading conspiracy theories about government censorship."

Massie went on to point to a tweet he posted May 19, 2021, under his official congressional account, in which he had linked to a peer-reviewed study that found the effectiveness of natural immunity was identical to that of the Pfizer COVID shot.

> *"Here's a comprehensive study that tracked reinfections and COVID complications for 187,549 people with prior SARS-CoV2 infection,"* he wrote in his tweet. *"Conclusion: Effectiveness of immunity due to prior infection is the same as for the Pfizer vaccine."*

This tweet was censored by Twitter after the Stanford Internet Observatory's Virality Project flagged it as "misinformation." As detailed in previous articles, the Virality Project is partnered with CISA and funded by the U.S. government to perform censorship activities the government cannot legally perform.

When asked if she thought there was a reason to flag Massey's tweet, Troye answered, "Depends on whether you're spreading inaccurate information." But who determines its "accuracy"?

It was a peer-reviewed, published study, which means several scientists who were not part of the study reviewed it. Is the Virality Project qualified to judge the accuracy of published research? This is a very dangerous slippery slope. If we cannot share peer-reviewed science, which is the epitome of "reputable source," then what, exactly, is acceptable to share?

> *"Are you going to sit here and maintain that it is a conspiracy theory that this occurred?"* Massey asked Troye. *"We have the documents ... that showed this [censorship] occurred."*
>
> *"Well, then it [Massey's tweet] must have been flagged for a reason,"* Troye replied.
>
> *"What reason?"* said Massey. *"Is there ever a good reason to censor a member of Congress? ... I bring this up, No. 1 to show that your testimony is false. But No. 2, if they can do this to a member of Congress' official account, they can do it to anybody."*

Whistleblower Reveals Military Contractors' Secret Plan for Censorship

Investigative journalist Michael Shellenberger testified at this meeting for the second time. Nine months ago, he testified and shared evidence with the Subcommittee about the existence of a "**Censorship Industrial Complex**, a network of government agencies, including the Department of Homeland Security, government contractors, and Big Tech media platforms that conspired to censor ordinary Americans and elected officials alike for holding disfavored views."[2]

All of that was wild enough, but there's more. At the November 30 hearing, Shellenberger exposed a group called the Cyber Threat Intelligence League (CTIL), which consists of military contractors that are not only censoring Americans, but also using sophisticated psychological operations against us.

According to Shellenberger, the CTIL was founded by a group of former Israeli and British intelligence agents who initially volunteered their cybersecurity services FOR FREE to multi-billion-dollar hospital and health care organizations in the U.S.

CTIL also offers physical security and "cognitive" security, i.e., protection against misinformation, and these services are volunteered by U.S. and British military contractors. According to a whistleblower who shared internal CTIL documents with Shellenberger, a number of CTIL "volunteers" are currently in government employ.

> **"The CTIL's plan to control the information landscape includes using debanking as financial leverage, pressuring social media platforms to change their terms of service to facilitate censorship and deplatforming under the guise of 'terms of service violations,' and more."**

They also used formal government letter head (FBI, CISA, U.S. Navy and so on) when communicating with each other. As noted by Massey, that "makes it hard for folks to claim that these weren't agents of the government or acting in coordination with the government ..."

CTIL Files Show Censorship Plot Is Bigger Than Imagined

Now, the CTIL's plan to control the information landscape goes further than those of CISA, the Virality Project and other government-led censorship activities. CTIL's plan also includes using debanking as financial leverage to shut people up, and pressuring

social media platforms to change their terms of service to facilitate censorship and deplatforming under the guise of "terms of service violations" — and more.

In a December 4, 2023, Substack article, Shellenberger's colleague, Alex Gutentag wrote about this new cache of documents, referred to as the CTIL Files:[3]

> *"During last Thursday's [November 30, 2023] Congressional hearing on the Weaponization of the Federal Government, Democratic members of Congress insisted[4] that censorship efforts of groups like the Cyber Threat Intelligence League (CTIL),[5] the Election Integrity Partnership (EIP),[6] and the Virality Project (VP)[7] were benign and not a violation of the First Amendment.*
>
> *'It's not the First Amendment!' said Rep. Dan Goldman, 'It's the [social media platforms'] Terms of Service ... And they are flagging it for the social media companies to make their own decisions. That is not the First Amendment. That is the Terms of Service.'*
>
> *But the CTIL Files, a trove of documents that a whistleblower provided to Public and Racket, reveal that US and UK military contractors developed and used advanced tactics — including demanding that social media platforms change their Terms of Service — to shape public opinion about Covid-19, and that getting content removed was just one strategy used by the Censorship Industrial Complex."*

Adversarial Misinformation and Influence Tactics and Techniques

As explained by Gutentag,[8] the CTIL partnered with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) to implement a framework called "AMITT," which stands for "Adversarial Misinformation and Influence Tactics and Techniques."

The predecessor to this program was the DISARM framework — described as an "open-source, community-led[9] ... master framework for fighting disinformation through sharing

data and analysis, and coordinating effective action[10]" — created by the DISARM Foundation in 2017.

According to the DISARM Foundation, AMITT was launched with the financial support of the Craig Newmark Philanthropies in 2019.[11,12] The AMITT framework includes a variety of "offensive actions," including:[13]

- Influencing government policy
- Discrediting alternative media
- Using bots and sock puppets to manipulate and direct public discussion
- Pre-bunking
- Counter-messaging

More specific AMITT strategies include but are not limited to:

Creating policy that forces social media to police mis- and disinformation
Creating "strong dialogue" between the federal government and private sector to improve reporting
Marginalizing and discrediting "extremists"
Naming and shaming "influencers" who share unsanctioned information
Simulating misinformation and disinformation campaigns, and responses to them, beforehand
Debanking offenders and cutting off their access to financial services[14]
"Inoculating" populations against "misinformation" using "media literacy training"

A Full-Fledged Military-Led Influence Operation

Gutentag continues:[15]

> *"Far from simply protecting the public from falsehoods, both government and non-profit actors within Censorship Industrial Complex have followed CTIL's exact playbook and have waged a full-fledged influence operation against Americans.*
>
> *This influence operation has deep ties to security and intelligence agencies, as is evidenced through many examples of collaboration. In one instance of such collaboration, supposedly independent "disinformation researchers" like Renée DiResta coordinated[16] a 2020 election tabletop exercise with military officials.*
>
> *Defense and intelligence funding supports much of the Censorship Industrial Complex. For instance, Graphika, which was involved in both EIP and VP, receives grants from the Department of Defense, DARPA, and the Navy.*
>
> *Pentagon-affiliated entities are heavily involved in 'anti-disinformation' work. Mitre, a major defense contractor, received funding to tackle 'disinformation' about elections and COVID.*
>
> *The US government paid Mitre, an organization staffed by former intelligence and military personnel, to monitor and report[17] what Americans said about the virus online, and to develop vaccine confidence messaging.[18]*
>
> *This government-backed military research group, Public discovered, was present in the EIP and VP misinformation reporting system, and in election disinformation report emails to CISA ...*
>
> *Why are agencies that are supposed to combat foreign threats using military-grade psychological tools to wage influence operations against the domestic population?"*

Anti-Democratic Ideology Is Driving the Censorship

As noted by Gutentag, these efforts appear to be partly driven by the need to manufacture perceived threats to justify the existence of the counter-terror bureaucracy." But there are also clear ideological factors at play. He writes:[19]

> *"Both [federal law enforcement and the intelligence community] now essentially treat Americans as an enemy population, with enormous support from the Democratic party and the legacy media.*
>
> *The result has been large-scale information warfare against US citizens, with sophisticated tactics being employed to develop propaganda narratives about Trump, COVID, and the 2020 election in the name of combatting 'disinformation.' We are now uncovering the clear evidence that military contractors appear to have been at the forefront of this effort ...*
>
> *What was once considered a 'conspiracy theory' that military and intelligence forces were manipulating public opinion through inorganic interventions, has now been confirmed.*
>
> *Our study of the Censorship Industrial Complex has exposed a far-reaching plan to subvert the democratic process and engage in activities that have a basis in military techniques and which are tantamount to attempts at thought or mind control."*

The Plan to Get Censorship Back on Twitter

The short clip above features Alex Stamos, head of the Stanford Internet Observatory, which runs the government's censorship apparatus via its Virality Project.

In it, he's taunting Elon Musk, saying he "bought himself into a hellish existence" by making moderating Twitter his personal responsibility. In so doing, Musk is placing his net worth, most of which is invested in Tesla, as well as all other Tesla shareholders, "in jeopardy."

The reason? Four words: The Digital Services Act.[20] This European Union law, which took effect August 25, 2023, requires online companies to actively police their platforms for "illegal" content or face huge fines — up to 6% of their global revenue. Repeated refusal to comply with rules or requests for action can result in suspension of the platform within the EU altogether.

What Stamos appears to be insinuating is that by Musk insisting on keeping X a free speech platform, he risks losing it all, and this kind of financial extortion leverage is precisely what the CTIL plan calls for.

Another Surveillance Program Revealed

In related news, Wired magazine recently reported[21] on leaked documents that verify the existence of a "secretive government program" that allows law enforcement to access trillions of phone records of Americans without a warrant.

In a recent letter to the Department of Justice, U.S. Sen. Ron Wyden challenged the legality of the program, which has been up and running for more than a decade. According to Wired:[22]

> *"... a surveillance program now known as Data Analytical Services (DAS) has for more than a decade allowed federal, state, and local law enforcement agencies to mine the details of Americans' calls, analyzing the phone records of countless people who are not suspected of any crime, including victims.*
>
> *Using a technique known as chain analysis, the program targets not only those in direct phone contact with a criminal suspect but anyone with whom those individuals have been in contact as well."*

DAS started out as a program called Hemisphere, run by the White House in coordination with AT&T. It was renamed DAS in 2013. It captures phone calls made using the AT&T infrastructure on behalf of U.S. law enforcement agencies, including local police, sheriffs' departments, U.S. customs and postal inspectors.

DAS is managed under an anti-drug trafficking program called HIDTA, which stands for "high-intensity drug trafficking area," but leaked files from the Northern California Regional Intelligence Center (NCRIC) shows the system is also being used in cases that are unrelated to drug trafficking. According to Wired, the DAS data does not include recordings of conversations.

The data do, however, include identifying information such as the names of the caller and recipient, their phone numbers, dates and times of calls, spanning at least 10 years or more into the past. Together, these data can be used to determine the exact locations of people, "a practice deemed unconstitutional without a warrant in 2018," Wired notes.

According to Wyden, "The scale of the data available to and routinely searched for the benefit of law enforcement under the Hemisphere Project is stunning in its scope." Moreover, it's not under congressional oversight, and because it's run out of the White House, it's exempt from privacy impact assessment rules and Freedom of Information Act (FOIA) requests.

Protections afforded by the Electronic Communications Privacy Act are also circumvented because AT&T's call record collection occurs along a telecommunications "backbone."

In early November 2023, Wyden and other lawmakers in the House and Senate introduced the Government Surveillance Reform Act of 2023,[23] which aims to patch the loopholes DAS is currently exploiting.

If passed, the DAS program would become explicitly illegal and would likely be forced to shut down. So, I encourage you to contact your representatives and ask them to support this legislation.

Sources and References

- [1] House Judiciary Committee on the Weaponization of the Federal Government
- [2] Public Substack November 30, 2023
- [3, 8, 13, 15, 19] Public Substack December 4, 2023
- [4] Public Substack December 1, 2023

- [5] Public Substack November 28, 2023
- [6] Public Substack November 7, 2023
- [7] Public Substack November 10, 2023
- [9] Disarm Foundation About Us
- [10, 11] Disarm Foundation DISARM Framework
- [12] Disarm Foundation Brief History
- [14] Disarm Framework C00129
- [16] Twitter NetworkAffects April 25, 2023
- [17] YouTube Mitre Squint
- [18] COVID-19 Health Communication Playbook (Archived)
- [20] Twitter Mike Benz December 4, 2023
- [21, 22] Wired November 28, 2023
- [23] Wired November 7, 2023