MERCOLA
Take Control of Your Health

How DARPA Took Over Pentagon Internet on Inauguration Day

Analysis by Dr. Joseph Mercola ✔ Fact Checked

STORY AT-A-GLANCE

- On inauguration day, Global Resource Systems LLC received control of tens of millions of Pentagon-owned IP addresses that were previously dormant
- The U.S. Department of Defense (DOD) made the mysterious transfer, and the number of DOD-owned IP addresses announced by Global Resource Systems increased from 56 million in late January to 175 million in April 2021
- This means the company now announces over 100 million more addresses than Comcast, the largest residential internet provider in the US
- Theories quickly emerged from the networking community about why an obscure company was handed so much of the Pentagon's internet; the Pentagon's Defense Digital Service (DDS) said it's a pilot project to defend against cyber-intrusions
- Raymond Saulino is the only name associated with the company, and he is also linked to Packet Forensics, a cybersecurity/internet surveillance equipment company with ties to the Pentagon's Defense Advanced Research Projects Agency (DARPA)
- The Pentagon built the internet as a tool for surveillance; if you're interested in learning more, I encourage you to read the book "Surveillance Valley: The Secret Military History of the Internet," by Yasha Levine

Just three minutes before Donald Trump left office on inauguration day, a "shadowy" company[1] called Global Resource Systems LLC received control of tens of millions of

Pentagon-owned IP addresses that were previously dormant.[2]

The U.S. Department of Defense (DOD) made the mysterious transfer, and the number of DOD-owned IP addresses announced by Global Resource Systems increased from 56 million in late January to 175 million in April 2021.[3]

“It is massive. That is the biggest thing in the history of the internet,” Doug Madory, director of internet analysis at network operating company Kentik, told The Associated Press, which conducted an investigation into the strange occurrence.[4] For reference, this swath of internet real estate amounts to one twenty-fifth of the current internet, and more than twice the size of internet being actively used by the Pentagon.[5]

Theories quickly emerged from the networking community about why an obscure company was handed so much of the Pentagon’s internet.

A Washington Post article suggested, "Did someone at the Defense Department sell off part of the military's vast collection of sought-after IP addresses as Trump left office? Had the Pentagon finally acted on demands to unload the billions of dollars’ worth of IP address space the military has been sitting on, largely unused, for decades?"[6,7]

Weeks went by before any explanations were provided, but the Pentagon’s response left more questions than answers.

Pentagon: ‘Pilot Effort’ to ‘Prevent Unauthorized Use’

The project is reportedly being run by the Pentagon’s Defense Digital Service (DDS), which was launched in 2015 to help the DOD “solve high-impact challenges” via “private-sector tools, approaches and talent.” Brett Goldstein, DDS director, stated:[8]

> *"DDS was created to bring in the best and brightest, to help advance the mission to solve some of our hardest technical problems, and to make sure technology doesn't get in the way of our mission: national defense. I think one of the things we've learned in government is that technology needs to enable the mission."*

In regard to the internet mystery, Goldstein said the "pilot project" intends to "assess, evaluate and prevent unauthorized use of DOD IP address space," and, according to the AP, "'identify potential vulnerabilities' as part of efforts to defend against cyber-intrusions by global adversaries, who are consistently infiltrating U.S. networks, sometimes operating from unused internet address blocks."[9]

Cybersecurity experts have suggested the IP addresses may be part of so-called "honeypots," which are intentionally vulnerable to attract hackers, or an effort to set up software and servers to monitor for suspicious activities.[10] According to Madory:[11]

> *"I interpret this to mean that the objectives of this effort are twofold. First, to announce this address space to scare off any would-be squatters, and secondly, to collect a massive amount of background internet traffic for threat intelligence."*

To get an idea of the scope of this pilot project and the many mysteries still behind it, Madory explained:[12]

> *"Following the increase, AS8003 [the entity announcing the DOD's internet space] became, far and away, the largest AS in the history of the internet as measured by originated IPv4 space. By comparison, AS8003 now announces 61 million more IP addresses than the now-second biggest AS in the world, China Telecom, and over 100 million more addresses than Comcast, the largest residential internet provider in the U.S.*
>
> *… While yesterday's statement from the DoD answers some questions, much remains a mystery. Why did the DoD not just announce this address space themselves instead of directing an outside entity to use the AS of a long dormant email marketing firm? Why did it come to life in the final moments of the previous administration?"*

The Company Has DARPA, Internet Surveillance Ties

Not much is known about Global Resource Systems, the company the Pentagon called upon to manage its address space, even though it has no record of government contracts. The AP revealed it has an address in Plantation, Florida, and was incorporated in Delaware and registered by a Beverly Hills lawyer.

Raymond Saulino is the only name associated with the company, however, and he is also linked to Packet Forensics, a cybersecurity/internet surveillance equipment company. According to the AP:[13]

> *"The company had nearly $40 million in publicly disclosed federal contracts over the past decade, with the FBI and the Pentagon's Defense Advanced Research Projects Agency [DARPA] among its customers …*
>
> *In 2011, Packet Forensics and Saulino, its spokesman, were featured in a Wired[14] story because the company was selling an appliance to government agencies and law enforcement that let them spy on people's web browsing using forged security certificates.*
>
> *The company continues to sell 'lawful intercept' equipment, according to its website. One of its current contracts with the Defense Advanced Research Projects Agency is for 'harnessing autonomy for countering cyber-adversary systems.' A contract description says it is investigating 'technologies for conducting safe, nondisruptive, and effective active defense operations in cyberspace.'*
>
> *Contract language from 2019 says the program would 'investigate the feasibility of creating safe and reliable autonomous software agencies that can effectively counter malicious botnet implants and similar large-scale malware.'"*

Adding even more confusion, a company by the same name — Global Resource Systems — and address was accused of sending email spam before it shut down more than 10 years ago.

Internet fraud researcher Ron Guilmette, who sued Global Resource Systems in 2006 for unfair business practices, told the AP, "It's deeply suspicious … If they wanted to be more

serious about hiding this they could have not used Ray Saulino and this suspicious name."[15]

DARPA Developed an Injectable Biosensor

DARPA has a long history of surveillance, including using medical and non-medical data to prevent terror attacks. DARPA managed Total Information Awareness (TIA), a program that sprang up after the 9/11 attacks that was seeking to collect Americans' medical records, fingerprints and other biometric data, along with DNA and records relating to personal finances, travel and media consumption.[16]

They also worked on the development of an injectable biosensor with its maker, Profusa.[17] The sensor allows a person's physiology to be examined at a distance via smartphone connectivity. Profusa is also backed by Google, the largest data mining company in the world.

Hydrogel is another DARPA invention, which involves nanotechnology and nanobots. This bioelectronic interface is part of the COVID-19 mRNA vaccines' delivery system. The biochip being developed by Profusa is similar to the proposed COVID-19 mRNA vaccines in that it utilizes hydrogel.

The implant is the size of a grain of rice, and connects to an online database that will keep track of changes in your biochemistry and a wide range of biometrics, such as heart and respiratory rate and much more.

Profusa said it intended to seek FDA approval for their tissue-integrating biosensor in 2021,[18] and a DARPA-backed study is also underway to measure early signs of influenza via the biosensor technology. The injectable sensors will be used to measure physiological statuses to reveal not only indicators of human response to infection but also "exposure to disease in healthy volunteers."[19]

A wireless patch that measures tissue oxygen levels would also be used, sending information to a mobile device for real-time data. According to Profusa, the biosensors may detect disease outbreaks, biological attacks and pandemics up to three weeks

earlier than current methods.[20] It would seem, however, that in order for such sensors to work on a widespread scale, extensive adoption would be required.

The Pentagon Created the Internet for Surveillance

While the internet is viewed as a tool to promote the dissemination of information, it was built by the government as a tool to spy on citizens. If you're interested in learning more about the little-known beginnings of the internet, I encourage you to read the book "Surveillance Valley: The Secret Military History of the Internet," by Yasha Levine.[21]

Levine, an investigative journalist, reveals that the internet began in the Vietnam-era and was used to spy on guerrilla fighters and antiwar protestors, "a military computer networking project that ultimately envisioned the creation of a global system of surveillance and prediction." What's more, the military surveillance objectives that underpinned the internet's development are still in force today.[22]

Consider Google, which **tracks your movements online**, even when you don't think you are using their products, because most websites you visit use the "free" Google Analytics program to track everything you do on a website.

Since the early 2000s, Google and Facebook in particular have been data mining online users. These data, then, have been applied to deep learning computers, giving them unprecedented ability to predict the type of messaging triggers that will create the maximum amount of fear — and **thus compliance**.

Silicon Valley Is Tied to US Intelligence Agencies

Silicon Valley remains deeply connected to U.S. intelligence agencies. Many suspect Facebook is the public-friendly version of DARPA's Lifelog, a database project aimed at tracking the minutiae of people's entire existence for national security surveillance purposes.[23] The Pentagon pulled the plug on Lifelog February 4, 2004, in response to backlash over privacy concerns.[24] Yet that same day, Facebook was launched.[25] Coincidence?

Google, Amazon, **Twitter** and other major tech companies are also tied to the "military-industrial-intelligence-media complex," to quote journalist Edward Curtin from Off-Guardian.[26] All provide invaluable surveillance and **censorship** functions, and without them, the **totalitarian control system** we now find ourselves caught in wouldn't be possible.

Even the U.S. Postal Service has apparently been monitoring Americans' social media posts via its United States Postal Inspection Service (USPIS) Internet Covert Operations Program (iCOP).[27] Echoing the trend of strangeness, Rachel Levinson-Waldman, deputy director of the Brennan Center for Justice's liberty and national security program, told Yahoo News, "This seems a little bizarre":[28]

> *"Based on the very minimal information that's available online, it appears that [iCOP] is meant to root out misuse of the postal system by online actors, which doesn't seem to encompass what's going on here. It's not at all clear why their mandate would include monitoring of social media that's unrelated to use of the postal system."*

A key solution will be decentralized platforms that not only virtually eliminate censorship but also foster privacy and free speech. What can you do to protect your privacy online right now? Here are a few suggestions:

- Switch from Facebook and Twitter to free-speech alternatives[29] such as Gab, MeWe, Minds and Parler.
- Switch from YouTube to uncensored alternatives[30] such as Bitchute, Brighteon, Banned.video and Thinkspot.
- Download the Signal or Telegram app to encrypt your text messages. Telegram also allows you to subscribe to channels (read-only messages are sent to your phone from any channel you subscribe. This feature is starting to be increasingly used by individuals who have been banned on other social media platforms).
- Use a VPN on your desktop, laptop and mobile devices to preserve your privacy.

For content creators and alternative news sources that no longer have a social media presence due to censoring, subscribe to their newsletter if available, and/or mark their website in your favorites and check back on a regular basis.

Boycott Google by avoiding any and all Google products:

- Stop using Google search engines. Alternatives include **DuckDuckGo**[31] and **SwissCows**.
- Uninstall Google Chrome and use **Brave** instead, available for all computers and mobile devices.[32] From a security perspective, Brave is far superior to Chrome and offers a free VPN service (virtual private network) to further **preserve your privacy**.
- Switch to a non-Google email service such as **ProtonMail**,[33] an encrypted email service based in Switzerland.
- Stop using Google docs. Digital Trends has published an article suggesting a number of alternatives.[34]
- Don't use Google Home devices. These devices record everything that occurs in your home, both speech and sounds such as brushing your teeth and boiling water, even when they appear to be inactive, and send that information back to Google. Android phones are also always listening and recording, as are Google's home thermostat Nest, and Amazon's Alexa.
- Ditch Fitbit, as it was recently purchased by Google and will provide them with all your physiological information and activity levels, in addition to everything else that Google already has on you.
- If you're a high school student, do not convert the Google accounts you created as a student into personal accounts.

Sources and Reference

- [1, 4, 9, 10, 13, 15] AP April 25, 2021

- [2, 3, 6] Ars Technica April 26, 2021
- [5] Zero Hedge April 26, 2021
- [7] The Washington Post April 24, 2021
- [8] U.S. Department of Defense, Defense Digital Service Delivers Mission-Aligned Tech for DOD May 29, 2019
- [11, 12] Kentik April 24, 2021
- [14] Wired March 24, 2018
- [16] Humans Are Free October 30, 2020
- [17] Bio Optics World May 25, 2016
- [18] Defense One March 3, 2020
- [19, 20] Profusa March 3, 2020
- [21, 22] SurveillanceValley.com
- [23] Military.com February 4, 2004
- [24] Rapture Ready FAQ: Lifelog project
- [25] History Facebook Launches February 4, 2004
- [26] Off-Guardian February 14, 2021
- [27, 28] Yahoo April 21, 2021
- [29, 30] Vision Launch 2020 List of Free Speech Social Media and Video Platforms
- [31] Fast Company, Inside DuckDuckGo
- [32] Opera Browser
- [33] ProtonMail
- [34] Digital Trends April 28, 2017