

# MUSCULAR (surveillance program)

**MUSCULAR (DS-200B)**, located in the United Kingdom,<sup>[1]</sup> is the name of a surveillance program jointly operated by Britain's Government Communications Headquarters (GCHQ) and the U.S. National Security Agency (NSA) that was revealed by documents released by Edward Snowden and interviews with knowledgeable officials.<sup>[2]</sup> GCHQ is the primary operator of the program.<sup>[1]</sup> GCHQ and the NSA have secretly broken into the main communications links that connect the data centers of Yahoo! and Google.<sup>[3]</sup> Substantive information about the program was made public at the end of October 2013.

## Contents

**Overview**

**Operational details**

**Reactions and countermeasures**

**Gallery**

**See also**

**References**

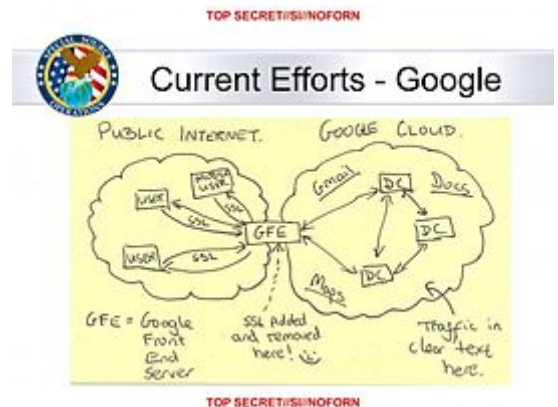
**External links**

## Overview

The programme is jointly run by:

- Government Communications Headquarters (GCHQ) (United Kingdom)
- U.S. National Security Agency (NSA)

MUSCULAR is one of at least four other similar programs that rely on a trusted 2nd party, programs which together are known as WINDSTOP. In a 30-day period from December 2012 to January 2013, MUSCULAR was responsible for collecting 181 million records. It was however dwarfed by another WINDSTOP program known (insofar) only by its code DS-300 and codename INCENSER, which collected over 14 billion records in the same period.<sup>[4]</sup>



## Operational details

According to the leaked document the NSA's acquisitions directorate sends millions of records every day from internal Yahoo! and Google networks to data warehouses at the agency's headquarters at Fort Meade, Maryland. The program operates via an access point known as **DS-200B**, which is outside the United States, and it relies on an unnamed telecommunications operator to provide secret access for the NSA and the GCHQ.<sup>[3]</sup>

According to the *Washington Post*, the MUSCULAR program collects more than twice as many data points ("selectors" in NSA jargon) compared to the better known PRISM.<sup>[2]</sup> Unlike PRISM, the MUSCULAR program requires no (FISA or other type of) warrants.

Closely related programmes are called INCENSER and TURMOIL. TURMOIL, belonging to the NSA, is a system for processing the data collected from MUSCULAR.<sup>[1]</sup>

According to a post-it style note from the presentation, the exploitation relied on the fact that (at the time at least) data was transmitted unencrypted inside Google's private cloud, with "Google Front End Servers" stripping and respectively adding back SSL from/to external connections. According to the *Washington Post*: "Two engineers with close ties to Google exploded in profanity when they saw the drawing." After the information about MUSCULAR was published by the press, Google announced that it was working on deploying encrypted communication between its datacenters.<sup>[2]</sup>

## Reactions and countermeasures

In early November 2013, Google announced that it was encrypting traffic between its data centers.<sup>[6]</sup> In mid-November, Yahoo! announced similar plans.<sup>[7]</sup>

In December 2013, Microsoft announced similar plans and used the expression "advanced persistent threat" in their press release (signed-off by their top legal representative), which the press immediately interpreted as comparison of the NSA with the Chinese government-sponsored hackers.<sup>[8][9]</sup>

## Gallery



Slide from NSA SSO presentation detailing the MUSCULAR capabilities	Internal NSA SSO update on the MUSCULAR operation, mentioning problem with Yahoo mailbox transfers, which required a throttling of data capture
---	---

## See also

- [2013 mass surveillance disclosures](#)
- [DISHFIRE](#), another NSA–GCHQ collaboration collecting SMS and similar messages worldwide
- [List of government mass surveillance projects](#)
- [Mass surveillance](#)
  - [Mass surveillance in the United Kingdom](#)
  - [Mass surveillance in the United States](#)
- Squeaky Dolphin, program targeting Facebook, YouTube, and Blogger

- STELLARWIND
- Total Information Awareness

## References

---

1. Gellman, Barton; Soltani, Ashkan; Peterson, Andrea (November 4, 2013). "How we know the NSA had access to internal Google and Yahoo cloud data" (<https://www.washingtonpost.com/blogs/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/>). *The Washington Post*. Retrieved November 5, 2013.
2. Gellman, Barton; Soltani, Ashkan (October 30, 2013). "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say" ([https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd\\_story.html](https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html)). *The Washington Post*. Retrieved October 31, 2013.
3. Gellman, Barton; DeLong, Matt. "How the NSA's MUSCULAR program collects too much data from Yahoo and Google" (<https://apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543/#document/p3/a129339>). *The Washington Post*. Retrieved 28 December 2013.
4. Gellman, Barton; DeLong, Matt (2013-10-30). "One month, hundreds of millions of records collected" (<https://apps.washingtonpost.com/g/page/world/one-month-hundreds-of-millions-of-records-collected/554/>). *The Washington Post*. Retrieved 2014-01-27.
5. Gallagher, Sean (October 31, 2013). "How the NSA's MUSCULAR tapped Google's and Yahoo's private networks" (<https://arstechnica.com/information-technology/2013/10/how-the-nsas-muscular-tapped-googles-and-yahoos-private-networks/>). *Ars Technica*. Retrieved November 1, 2013.
6. Gallagher, Sean (2013-11-06). "Googlers say "F\*\*\* you" to NSA, company encrypts internal network" (<https://arstechnica.com/information-technology/2013/11/googlers-say-f-you-to-nsa-company-encrypts-internal-network/>). *Ars Technica*. Retrieved 2014-01-15.
7. Bandom, Russell (2013-11-18). "Yahoo plans to encrypt all internal data by early 2014 to keep the NSA out" (<http://www.theverge.com/2013/11/18/5118150/yahoo-ceo-marissa-mayer-plans-to-encrypt-data-against-nsa-by-2014>). *The Verge*. Retrieved 2014-01-27.
8. Danny Yadron (2013-12-05). "Microsoft Compares NSA to 'Advanced Persistent Threat' - Digits - WSJ" (<https://blogs.wsj.com/digits/2013/12/05/microsoft-compares-nsa-to-advanced-persistent-threat/>). *Blogs.wsj.com*. Retrieved 2014-01-15.
9. Tom Warren (2013-12-05). "Microsoft labels US government a 'persistent threat' in plan to cut off NSA spying" (<http://www.theverge.com/2013/12/5/5177554/microsoft-plans-server-encryption-against-nsa-snooping>). *The Verge*. Retrieved 2014-01-15.

## External links

---

- Savage, Charlie; Miller, Claire; Perlroth, Nicole (October 30, 2013). "N.S.A. Said to Tap Google and Yahoo Abroad" (<https://www.nytimes.com/2013/10/31/technology/nsa-is-mining-google-and-yahoo-abroad.html>). *The New York Times*. Retrieved November 1, 2013.
- Rushe, Dominic; Ackerman, Spencer; Ball, James (October 30, 2013). "Reports that NSA taps into Google and Yahoo data hubs infuriate tech giants" (<https://www.theguardian.com/technology/2013/oct/30/google-reports-nsa-secretly-intercepts-data-links>). *The Guardian*. Retrieved November 2, 2013.
- Gellman, Barton; Soltani, Ashkan; Lindeman, Todd (October 30, 2013). "How the NSA is infiltrating private networks" (<https://apps.washingtonpost.com/g/page/national/the-nsa-is-hacking-private-networks/542/>). *The Washington Post*. Retrieved November 1, 2013.
- Miller, Claire (October 31, 2013). "Angry Over U.S. Surveillance, Tech Giants Bolster Defenses" ([https://www.nytimes.com/2013/11/01/technology/angry-over-us-surveillance-tech-giants-bolster-defenses.html?hp&\\_r=1&pagewanted=all&\\_](https://www.nytimes.com/2013/11/01/technology/angry-over-us-surveillance-tech-giants-bolster-defenses.html?hp&_r=1&pagewanted=all&_)). *The New York Times*. Retrieved November 1, 2013.
- Schneier, Bruce (October 31, 2013). "NSA Eavesdropping on Google and Yahoo Networks" ([https://www.schneier.com/blog/archives/2013/10/nsa\\_eavesdroppi\\_2.html](https://www.schneier.com/blog/archives/2013/10/nsa_eavesdroppi_2.html)). *Schneier on Security*. Retrieved November 1, 2013.
- Perlroth, Nicole; Markoff, John (November 25, 2013). "N.S.A. May Have Penetrated Internet Cable Links" ([https://www.nytimes.com/2013/11/26/technology/a-peephole-for-the-nsa.html?hp&\\_r=0&pagewanted=all](https://www.nytimes.com/2013/11/26/technology/a-peephole-for-the-nsa.html?hp&_r=0&pagewanted=all)). *The New York Times*. Retrieved November 26, 2013.
- Gellman, Barton; DeLong, Matt. "What Yahoo and Google did not think the NSA could see" (<https://apps.washingtonpost.com/g/page/world/what-yahoo-and-google-did-not-think-the-nsa-could-see/555/>). *The Washington Post*.

Retrieved March 14, 2014.

---

Retrieved from "[https://en.wikipedia.org/w/index.php?title=MUSCULAR\\_\(surveillance\\_program\)&oldid=870652705](https://en.wikipedia.org/w/index.php?title=MUSCULAR_(surveillance_program)&oldid=870652705)"

---

**This page was last edited on 26 November 2018, at 05:21 (UTC).**

Text is available under the [Creative Commons Attribution-ShareAlike License](#); additional terms may apply. By using this site, you agree to the [Terms of Use](#) and [Privacy Policy](#). Wikipedia® is a registered trademark of the [Wikimedia Foundation, Inc.](#), a non-profit organization.