

Operation Trojan Shield

Operation Trojan Shield (stylized TRØJAN SHIELD), part of **Operation Ironside**, was a collaboration by [law enforcement agencies](#) from several countries, running between 2018 and 2021. It was a [sting operation](#) that intercepted millions of messages sent through the supposedly secure [smartphone-based proprietary messaging app ANOM](#) (also stylized as **ANOM** or **ANØM**). The ANOM service was widely used by criminals, but instead of providing [secure communication](#), it was actually a [trojan horse](#) covertly distributed by the United States [Federal Bureau of Investigation](#) (FBI) and the [Australian Federal Police](#) (AFP), enabling them to monitor all communications. Through collaboration with other law enforcement agencies worldwide, the operation resulted in the arrest of over 800 suspects allegedly involved in criminal activity in 16 countries. Among the arrested people were alleged members of Australian-based [Italian mafia](#), [Albanian organised crime](#), [outlaw motorcycle clubs](#), drug [syndicates](#) and other [organised crime](#) groups.

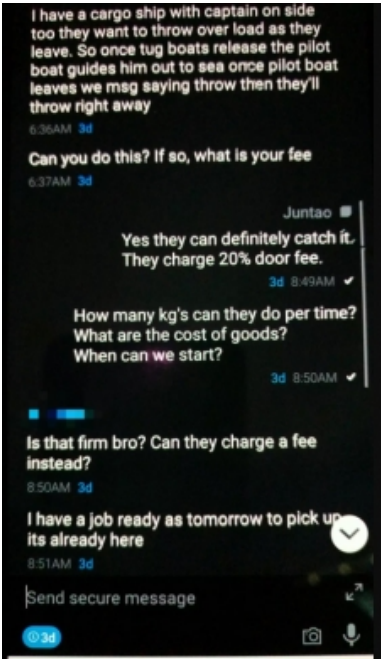
Background

An investigation into a Canadian secure messaging company called [Phantom Secure](#) was initiated in 2017. The FBI alleges that the investigation revealed that Phantom Secure sold its encrypted devices exclusively to members of transnational criminal organizations (TCO). Hardened encrypted devices provide an "impenetrable shield against law enforcement surveillance" and are in high demand by TCOs, thus the shutdown of [Phantom Secure](#) in March 2018 left a vacuum for TCOs in need of an alternative system for secure communication.

Around the same time, the [San Diego](#) FBI branch had been working with a person, known by the pseudonym "Afgoo",^[4] who had been developing a "next-generation" encrypted device for use by criminal networks. The person was facing charges and cooperated with the FBI in exchange for a reduced sentence. The person offered to develop ANOM and then use his contacts to distribute it to TCOs through existing networks.^{[5][6]} Before the devices were put to use, however, the FBI, and the AFP had a [backdoor](#) built into the communication platform which allowed law enforcement agencies to decrypt and store the messages as the messages were transmitted. The first communication devices with ANOM were offered by this informant to three former distributors of Phantom Secure in October 2018.^[7]

The FBI named the operation "Trojan Shield",^[8] and the AFP named it "Ironside".^[9] Europol set up the Operational Task Force Greenlight.^[10]




Distribution and usage



ANOM app screenshot

The ANOM devices consisted of a messaging app running on [Android](#) smartphones with a custom ROM called ArcaneOS that had been specially modified to disable normal functions such as [voice telephony](#), [email](#), or [location services](#), and with the addition of PIN entry screen scrambling to randomise the layout of the numbers, the deletion of all information on the phone if a specific PIN is entered, and the option for the automatic deletion of all information if unused for a specific period of time.^[11]

The app was opened by entering a specific calculation within the calculator app, described by the developer of [GrapheneOS](#) as "quite amusing security theater",^[11] where the messaging app then communicated with other devices via supposedly secure [proxy servers](#), which also – unbeknownst to the app's users – copied all sent messages to servers controlled by the FBI. The FBI could then decrypt the messages with a

Operation Trojan Shield	
Part of Operation Ironside	
<div></div> <p>ANOM app logo (top), the seal of the FBI's Operation Trojan Shield (bottom left), and the logo of the AFP's Operation Ironside (bottom right)</p>	
Operation name	Operation Trojan Shield
Part of	Operation Ironside
Roster	
Planned by	U.S. Federal Bureau of Investigation, United States Attorney's Office for the Southern District of California, Europol, Australian Federal Police, and others
Executed by	United States, Australia, Europol+
Countries participating	Sweden, United States, Australia, United Kingdom, New Zealand, Germany, Netherlands,

private key associated with the message, without ever needing physical access to the devices.^{[6][12]} The devices also had a fixed identification number assigned to each user, allowing messages from the same user to be connected to each other.^[12]

About 50 devices were distributed in Australia for beta testing from October 2018. The intercepted communications showed that every device was used for criminal activities, primarily being used by organised criminal gangs.^[6] About 125 devices were shipped to different drop-off points to the United States in 2020.^[13]

Use of the app spread through word of mouth,^[6] and was also encouraged by undercover agents;^[14] drug trafficker Hakan Ayik was identified "as someone who was trusted and was going to be able to successfully distribute this platform", and without his knowledge was encouraged by undercover agents to use and sell the devices on the black market, further expanding its use.^{[14][15]} After users of the devices requested smaller and newer phones, new devices were designed and sold; customer service and technical assistance was also provided by the company.^{[7][11]} The most commonly used languages on the app were Dutch, German and Swedish.^[16]

After a slow start, the rate of distribution of ANOM increased from mid-2019. By October 2019, there were several hundred users. By May 2021, there had been 11,800 devices with ANOM installed, of which about 9,000 were in use. New Zealand had 57 users of the ANOM communication system.^[3] The Swedish Police

No. of countries participating	16
Mission	
Target	organized criminal networks that use encrypted communication devices
Objective	Surveillance of criminal activity
Method	Honeypot communication device with security backdoor
Timeline	
Date begin	2018
Date end	2021
Date executed	<ul style="list-style-type: none"> October 2018 (initial device distribution) 8 June 2021 (search warrant execution)
Results	
Suspects	Germany: 150
Arrests	1,119+ <ul style="list-style-type: none"> Europol: 800+ Australia: 224 New Zealand: 35 Germany: 60+

had access to conversations from 1,600 users, of which they focused their surveillance on 600 users.^[17] [Europol](#) stated 27 million messages were collected from ANOM devices across over 100 countries.^[18]

Some skepticism of the app did exist; one WordPress blog post in March 2021 called the app a scam.^{[19][20][6]}

Law enforcement operational methodology

The following is alleged by the FBI:

2018

The "backdoor" built by the FBI into the system by design would send an additional encrypted copy of each message sent by the ANOM users to a third party server referred to by the FBI as an "iBot" server. Fourth amendment interpretations endangered the project if the iBot servers were located in the U.S. and so the servers necessarily were located outside U.S. borders. The first server would decrypt the copied message, process the information in the message (GPS location, text, username/Jabber-ID, password etc.) and then re-encrypt it to send it to a second "FBI-owned" iBot server.

2019

Because the FBI could not own the first iBot node, nor were they permitted to receive any of the seized information about U.S. citizens, they contracted with the AFP to run the first node of the server and process the data. (Australian law does not provide the same protections as U.S. law for its citizens.) Controversially the AFP *did* share "general" information about conversations from the

Miscellaneous results

- 40 tons of drugs (over eight tons of cocaine, 22 tons of cannabis and cannabis resin, six tons of synthetic drug precursors, two tons of synthetic drugs), 250 guns, 55 luxury cars,^[1] more than \$48 million in various currencies and cryptocurrencies.
- Australia: 104 firearms, \$45 million AUD.
- New Zealand: \$3.7 million in assets, including 14 vehicles, drugs, firearms and more than \$1 million in cash.^{[2][3]}

ANOM messages with the FBI during this time period despite Australia's judicial order to intercept ANOM communications did *not* allow for the sharing of the content with foreign partners.

Summer 2019

Allegedly, the FBI officially had not reviewed any of the ANOM decrypted content yet by the summer of 2019. As a method of getting around the Australian court order, the FBI needed to secure a [mutual legal assistance treaty](#) (MLAT) request with a third country where the transfer of information would be legal pursuant to their national laws. While much work was done to keep the identity of the third country secret, its identity was discovered by the press as Lithuania in 2023.^[21]

The FBI worked with Lithuania through the Autumn of 2019. However, the FBI alleges that the iBots had geo-fenced all messages that *originated* from the U.S., to prevent the FBI-owned iBot2 server from inadvertently seizing messages in violation of the Fourth Amendment.

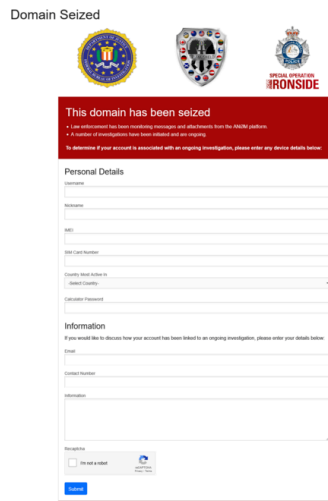
7 October 2019 – 7 January 2020

Lithuania created an iBOT copy (iBot3) of the FBI-owned iBOT2 server and began receiving content from the iBOT2 server every 2–3 days.

Post 7 January 2020

A newer MLAT and court order from Lithuania allowed the FBI to receive ANOM user data every Monday, Wednesday and Friday until 7 June 2021. This encompasses all data ever generated by any ANOM user with the alleged exception of 15 (or 17) users that originated from phones in the U.S.

Arrests and reactions



ANOM website screenshot, 10 June 2021

The sting operation culminated in [search warrants](#) that were executed simultaneously around the globe on 8 June 2021.^[3] It is not entirely clear why this date was chosen, but news organisations have speculated it might be related to a warrant for server access expiring on 7 June.^[6] It has also been speculated that the date was chosen due to an anonymous blog post – *Anom Exposed*^[22] – published on 29th of March 2021, in which Anom's alleged security was put into question.^[23] The background to the sting operation and its transnational nature was revealed following the execution of the search warrants. Over 800 people were arrested in 16 countries.^{[24][25][1]} Among the arrested people were alleged members of Australian-based [Italian mafia](#), [Albanian organised crime](#), [outlaw motorcycle gangs](#), drug [syndicates](#) and other crime groups.^{[24][9][26]} In the [European Union](#), arrests were coordinated through [Europol](#).^[27] Arrests were also made in the United Kingdom, although the [National Crime Agency](#) was unwilling to provide details about the number arrested.^[28]

The seized evidence included almost 40 tons of drugs (over eight tons of cocaine, 22 tons of cannabis and cannabis resin, six tons of synthetic drug precursors, two tons of synthetic drugs), 250 guns, 55 luxury cars,^[1] and more than \$48 million in various currencies and cryptocurrencies. In Australia, 224 people were arrested on 526 total charges.^[26] In New Zealand, 35 people were arrested and faced a total of 900 charges. Police seized \$3.7 million in assets, including 14 vehicles, drugs, firearms and more than \$1 million in cash.^{[2][3]}

Over the course of the three years, more than 9,000 police officers across 18 countries were involved in the sting operation. Australian Prime Minister [Scott Morrison](#) said that the sting operation had "struck a heavy blow against organised crime". Europol described it as the "biggest ever law enforcement operation against encrypted communication".^[24]

In 2022, [Motherboard](#) journalist [Joseph Cox](#) published documents stating that the FBI obtained message data through the cooperation of an unnamed country within the [European Union](#).^[29]

Australia

About 50 of the devices had been sold in Australia. Australian Federal Police arrested 224 suspects and seized 104 firearms and confiscated cash and possessions valued at more than 45 million AUD.^[30]

Germany

In Germany, the majority of the police activity was in the state of [Hesse](#) where 60 of the 70 nationwide suspects were arrested.^[31] Police searched 150 locations and in many cases under suspicion of drug trafficking.^[32]

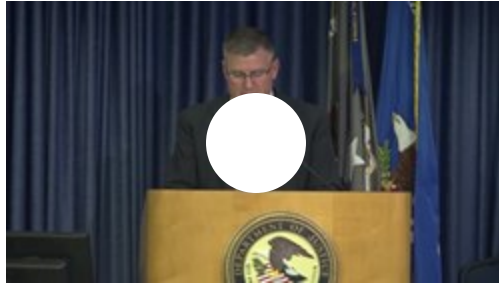
Netherlands

In the Netherlands, 49 people were arrested by [Dutch National Police](#) while they investigated 25 drug production facilities and narcotics caches. Police also seized eight firearms, large supplies of narcotics and more than 2.3 million euro.^[16]

Sweden

In Sweden, 155 people were arrested as part of the operation.^[17] According to police in Sweden which received intelligence from the FBI, during an early phase of the operation it was discovered that many of the suspects were in Sweden. [Linda Staaf](#), head of the Swedish police's intelligence activities, said that "Sweden's users stood out in that there was a higher rate of violent crime linked to Sweden".^[33]

United States



Press conference announcing the
Operation Trojan Shield arrests

The first search warrants were granted by judges in May 2021. Initially, no arrests were made in the United States because of 4th amendment interpretations that prevented law enforcement from collecting messages from domestic subjects.^[34] However, the [United States Department of Justice](#) indicted seventeen persons (all foreign nationals, see [court dockets here \(https://www.courtlistener.com/tags/spiritguide/operation-trojan-shield/\)](https://www.courtlistener.com/tags/spiritguide/operation-trojan-shield/)) under the [Racketeer Influenced and Corrupt Organizations Act](#) for their participation in "the ANOM enterprise" which spread the devices.^[35]

Legal challenges

As of April 2023, multiple court cases have been brought in Australia to challenge the legitimacy of the ANOM sting operation. A judgment in one of the cases before the [Supreme Court of South Australia](#) has ruled in favor of the police,^[36] although that judgment has, since November 2023, been appealed.^{[37][38]}

See also

- [EncroChat](#) – a network infiltrated by law enforcement to investigate [organized crime](#) in Europe
- [Ennetcom](#) – a network seized by Dutch authorities, who used it to make arrests
- [Sky Global](#) – a communications network and service provider based in Vancouver, Canada

References

1. Svetlova, Anna (8 June 2021). [Европол задержал более 800 преступников в рамках международной операции \(https://www.gazeta.ru/social/news/2021/06/08/n_16076948.shtml\)](https://www.gazeta.ru/social/news/2021/06/08/n_16076948.shtml) [Europol detained over 800 criminals as part of an international operation] (in Russian). [Gazeta.ru](https://www.gazeta.ru). Archived (<https://web.archive.org/web/20210609034451/https://www.gazeta.ru/so>

cial/news/2021/06/08/n_16076948.shtml) from the original on 9 June 2021. Retrieved 8 June 2021.

2. Corder, Mike; Perry, Nick (8 June 2021). "FBI-encrypted app hailed as a 'shining example' of collaboration between world cops for tricking gangs" (<https://www.stuff.co.nz/national/crime/300327974/fbiencrypted-app-hailed-as-a-shining-example-of-collaboration-between-world-cops-for-tricking-gangs>) . *Stuff*. Archived (<https://web.archive.org/web/20210609034451/https://www.stuff.co.nz/national/crime/300327974/fbiencrypted-app-hailed-as-a-shining-example-of-collaboration-between-world-cops-for-tricking-gangs>) from the original on 9 June 2021. Retrieved 8 June 2021.
3. "Anom: The app at the heart of the FBI's major transnational sting" (<https://www.nzherald.co.nz/nz/anom-the-app-at-the-heart-of-the-fbis-major-transnational-sting/HUPSM4FPQT2KZCBSVAUINWA2GE/>) . *The New Zealand Herald*. 8 June 2021. Archived (<https://web.archive.org/web/20210609034449/https://www.nzherald.co.nz/nz/anom-the-app-at-the-heart-of-the-fbis-major-transnational-sting/HUPSM4FPQT2KZCBSVAUINWA2GE/>) from the original on 9 June 2021. Retrieved 8 June 2021.
4. Cox, Joseph. "Inside the Biggest FBI Sting Operation in History" (<https://www.wired.com/story/inside-biggest-fbi-sting-operation-in-history/>) . *Wired*. ISSN 1059-1028 (<https://search.worldcat.org/issn/1059-1028>) . Retrieved 4 February 2025.
5. Corder, Mike; Perry, Nick; Spagat, Elliot (8 June 2021). "Global sting began by creating message service for crooks" (<https://apnews.com/article/europe-technology-a6ac691e26be2efc6e2f4a6974117536>) . *AP NEWS*. Archived (<https://web.archive.org/web/20210608103515/https://apnews.com/article/europe-technology-a6ac691e26be2efc6e2f4a6974117536>) from the original on 8 June 2021. Retrieved 6 April 2023.
6. "ANOM global phone sting: What we know" (<https://www.rte.ie/news/2021/0608/1226913-global-crime/>) . Raidió Teilifís Éireann. Agence France-Presse. 8 June 2021. Archived (<https://web.archive.org/web/20210609034448/https://www.rte.ie/news/2021/0608/1226913-global-crime/>) from the original on 9 June 2021. Retrieved 8 June 2021.
7. Zhuang, Yan; Peltier, Elia; Feuer, Alan (8 June 2021). "The Criminals Thought the Devices Were Secure. But the Seller Was the F.B.I." (<https://www.nytimes.com/2021/06/08/world/australia/operation-trojan-horse-anom.html>) *The New York Times*. ISSN 0362-4331 (<https://search.worldcat.org/issn/0362-4331>) . Archived (<https://web.archive.org/web/20210609014628/https://www.nytimes.com/2021/06/08/world/australia/operation-trojan-horse-anom.html>) from the original on 9 June 2021. Retrieved 8 June 2021.

8. Harding, Luke (8 June 2021). "Hundreds arrested in global crime sting after underworld app is hacked" (<https://www.theguardian.com/australia-news/2021/jun/08/anom-encrypted-app-fbi-afp-australia-federal-police-sting-operation-ironside-an0m>) . *The Guardian*. Archived (<https://web.archive.org/web/20210609034518/https://www.theguardian.com/australia-news/2021/jun/08/anom-encrypted-app-fbi-afp-australia-federal-police-sting-operation-ironside-an0m>) from the original on 9 June 2021. Retrieved 8 June 2021.
9. Westcott, Ben. "FBI and Australian Federal Police encrypted app trap ensnares hundreds of criminal suspects" (<https://www.cnn.com/2021/06/08/australia/afp-fbi-anom-app-operation-ironside/index.html>) . CNN. Archived (<https://web.archive.org/web/20210609005546/https://www.cnn.com/2021/06/08/australia/afp-fbi-anom-app-operation-ironside/index.html>) from the original on 9 June 2021. Retrieved 8 June 2021.
10. Europol (<https://twitter.com/Europol/status/1402115313559388164>) on Twitter
11. Cox, Joseph (8 July 2021). "We Got the Phone the FBI Secretly Sold to Criminals" (<https://www.vice.com/en/article/anom-phone-arcaneos-fbi-backdoor/>) . *Vice*. Retrieved 8 July 2021.
12. Robertson, Adi (8 June 2021). "The FBI secretly launched an encrypted messaging system for criminals" (<https://www.theverge.com/2021/6/8/22524307/anom-encrypted-messaging-fbi-europol-afp-sting-operation-trojan-shield-greenlight>) . *The Verge*. Archived (<https://web.archive.org/web/20210609013810/https://www.theverge.com/2021/6/8/22524307/anom-encrypted-messaging-fbi-europol-afp-sting-operation-trojan-shield-greenlight>) from the original on 9 June 2021. Retrieved 8 June 2021.
13. Cox, Joseph (12 January 2022). "FBI Honeypot Phone Company Anom Shipped Over 100 Phones to the United States" (<https://www.vice.com/en/article/fbi-anom-shipped-100-phones-united-states/>) . *Vice*. Retrieved 12 January 2022.
14. Taouk, Maryanne (8 June 2021). "Underworld figure Hakan Ayik unwittingly helped Operation Ironside, the AFP's biggest criminal sting" (<https://www.abc.net.au/news/2021-06-09/fugitive-hakan-ayik-unwittingly-helped-operation-ironside/100198164>) . Australian Broadcasting Corporation. Archived (<https://web.archive.org/web/20210609034449/https://www.abc.net.au/news/2021-06-09/fugitive-hakan-ayik-unwittingly-helped-operation-ironside/100198164>) from the original on 9 June 2021. Retrieved 8 June 2021.
15. "Hakan Ayik: The man who accidentally helped FBI get in criminals' pockets" (<https://www.bbc.com/news/world-57397779>) . *BBC News*. 8 June 2021. Archived (<https://web.archive.org/web/20210608184123/https://www.bbc.com/news/world-57397779>) from the original on 8 June 2021. Retrieved 8 June 2021.

16. "49 NL arrests in international 'encrypted phones' operation" (<https://nltimes.nl/2021/06/08/49-nl-arrests-international-encrypted-phones-operation>) . *NL Times*. 8 June 2021. Retrieved 10 June 2021.
17. Smed, Akvelina (8 June 2021). "155 tungt kriminella gripna i Sverige i stor insats" (<https://www.svt.se/nyheter/inrikes/europol-berattar-om-det-omfattande-tillslaget>) [155 serious criminals arrested in Sweden in large operation]. *SVT Nyheter* (in Swedish). Archived (<https://web.archive.org/web/20210609034449/https://www.svt.se/nyheter/inrikes/europol-berattar-om-det-omfattande-tillslaget>) from the original on 9 June 2021. Retrieved 8 June 2021.
18. Chappell, Bill (8 June 2021). "Drug Rings' Favorite New Encrypted Platform Had One Flaw: The FBI Controlled It" (<https://www.npr.org/2021/06/08/1004332551/drug-rings-platform-operation-trojan-shield-anom-operation-greenlight>) . *NPR*. Archived (<https://web.archive.org/web/20210609034455/https://www.npr.org/2021/06/08/1004332551/drug-rings-platform-operation-trojan-shield-anom-operation-greenlight>) from the original on 9 June 2021. Retrieved 8 June 2021.
19. "ANOM Encrypted Scam Exposed" (<https://web.archive.org/web/20210610004653/http://webcache.googleusercontent.com/search?q=cache%3Ahttps%3A%2F%2Fanomexposed.wordpress.com%2F2021%2F03%2F29%2Fanom-encrypted-scam-exposed%2F>) . *ANOM Exposed*. Archived from the original (<https://anomexposed.wordpress.com/2021/03/29/anom-encrypted-scam-exposed/>) on 10 June 2021. Retrieved 13 June 2021.
20. "Anom Encrypted App Analysis" (<https://the-latest.news/anom-encrypted-app-analysis/>) . 9 June 2021. Archived (<https://web.archive.org/web/20210609010314/https://the-latest.news/anom-encrypted-app-analysis/>) from the original on 9 June 2021. Retrieved 9 June 2021.
21. Cox , Joseph (11 September 2023). "Revealed: The Country that Secretly Wiretapped the World for the FBI" (<https://www.404media.co/revealed-the-country-that-secretly-wiretapped-the-world-for-the-fbi/>) . *404 Media*.
22. "ANOM EXPOSED" (<https://anomexposed.wordpress.com/>) . *ANOM EXPOSED*. 10 June 2021.
23. "Anom encrypted scam exposed" (https://archive.today/20210607210421/https://webcache.googleusercontent.com/search?q=cache:PwQXt6Sn_YwJ:https://anomexposed.wordpress.com/) . Archived from the original (https://webcache.googleusercontent.com/search?q=cache:PwQXt6Sn_YwJ:https://anomexposed.wordpress.com/) on 7 June 2021.
24. "ANOM: Hundreds arrested in massive global crime sting" (<https://www.bbc.com/news/world-57394831>) . *BBC News*. 8 June 2021. Archived (<https://web.archive.org/web/20210608054245/https://www.bbc.com/news/world-57394831>) from the original on 8 June 2021. Retrieved 8 June 2021.

25. Cox, Joseph (8 June 2021). "Trojan Shield: How the FBI Secretly Ran a Phone Network for Criminals" (<https://www.vice.com/en/article/operation-trojan-shield-anom-fbi-secret-phone-network/>) . *Vice*. Archived (<https://web.archive.org/web/20210608031704/https://www.vice.com/en/article/akgkwj/operation-trojan-shield-anom-fbi-secret-phone-network>) from the original on 8 June 2021. Retrieved 8 June 2021.
26. "AFP-led Operation Ironside smashes organised crime" (<https://www.afp.gov.au/news-media/media-releases/afp-led-operation-ironside-smashes-organised-crime>) (Press release). Australian Federal Police. 8 June 2021. Archived (<https://web.archive.org/web/20210608025117/https://www.afp.gov.au/news-media/media-releases/afp-led-operation-ironside-smashes-organised-crime>) from the original on 8 June 2021. Retrieved 8 June 2021.
27. "Trojan Shield: Europol details massive organized crime sting" (<https://www.dw.com/en/trojan-shield-europol-details-massive-organized-crime-sting/a-57808917>) . Deutsche Welle. 8 June 2021. Archived (<https://web.archive.org/web/20210609034451/https://www.dw.com/en/trojan-shield-europol-details-massive-organized-crime-sting/a-57808917>) from the original on 9 June 2021. Retrieved 8 June 2021.
28. Davis, Margaret. "UK criminals among those duped into using secret message service run by the FBI" (<https://www.belfasttelegraph.co.uk/news/uk/uk-criminals-among-those-duped-into-using-secret-message-service-run-by-the-fbi-40514540.html>) . *Belfast Telegraph*. ISSN 0307-1235 (<https://search.worldcat.org/issn/0307-1235>) . Archived (<https://web.archive.org/web/20210609034450/https://www.belfasttelegraph.co.uk/news/uk/uk-criminals-among-those-duped-into-using-secret-message-service-run-by-the-fbi-40514540.html>) from the original on 9 June 2021. Retrieved 8 June 2021.
29. Cox, Joseph (3 June 2022). "A European Country Helped the FBI Intercept Anom Messages, But It Wants to Remain Hidden" (<https://www.vice.com/en/article/anom-third-country-europe-european-union-fbi/>) . *Vice*. Retrieved 3 June 2022.
30. "Checks and balances needed for new police surveillance powers" (<https://www.smh.com.au/politics/federal/checks-and-balances-needed-for-new-police-surveillance-powers-20210609-p57zm5.html>) . *The Sydney Morning Herald*. 9 June 2021. Retrieved 11 June 2021.
31. "Nach Europol-Razzia: Verdächtige in Untersuchungshaft" (https://www.welt.de/newsticker/dpa_nt/afxline/topthemen/article231682935/Nach-Europol-Razzia-Verdaechtige-in-Untersuchungshaft.html) [After Europol raid: Suspects in custody]. *Die Welt* (in German). 9 June 2021. Retrieved 10 June 2021.

32. "Nach Europol-Razzia: Dutzende Beschuldigte in Deutschland" (https://web.archive.org/web/20210611193023/https://www.saarbruecker-zeitung.de/nachrichten/politik/topthemen/nach-europol-razzia-dutzende-beschuldigte-in-deutschland_aid-59143575) [After Europol raid: dozens of suspects in Germany]. *saarbruecker-zeitung.de* (in German). 9 June 2021. Archived from the original (https://www.saarbruecker-zeitung.de/nachrichten/politik/topthemen/nach-europol-razzia-dutzende-beschuldigte-in-deutschland_aid-59143575) on 11 June 2021. Retrieved 10 June 2021.
33. Smed, Akvelina; Jönsson, Oskar; Boati, David (8 June 2021). "Underrättelsechefen: 'Sveriges användare stack ut'" (<https://www.svt.se/nyheter/inrikes/underrattelsechefen-sveriges-anvandare-stack-ut>) [The head of intelligence: 'Sweden's users stood out']. *SVT Nyheter* (in Swedish). Archived (<https://web.archive.org/web/20210610023020/https://www.svt.se/nyheter/inrikes/underrattelsechefen-sveriges-anvandare-stack-ut>) from the original on 10 June 2021. Retrieved 9 June 2021.
34. Malone, Ursula (14 June 2021). "The FBI played a huge role in Operation Ironside but haven't made a single arrest – here's why" (<https://www.abc.net.au/news/2021-06-15/no-one-in-america-arrested-in-operation-ironside/100213036>) . *ABC News*. Retrieved 15 June 2021.
35. Cox, Joseph (9 June 2021). "DOJ Charges Criminal 'Influencers' Who Worked for FBI's Honeypot Phone Company" (<https://www.vice.com/en/article/doj-charges-anom-influencers-fake-honeypot-company/>) . *Vice*. Retrieved 23 May 2022.
36. "Why accused criminals are challenging evidence from one of the world's biggest police stings" (<https://www.abc.net.au/news/2023-04-18/accused-criminals-challenge-anom-app-evidence-in-supreme-court/102107344>) . *ABC News*. 17 April 2023. Retrieved 18 April 2023.
37. Mott, Mitch (17 November 2023). "The argument that could bring Operation Ironside tumbling down" (<https://www.couriermail.com.au/news/south-australia/court-of-appeal-begins-australias-first-operation-ironside-anom-messages-question-of-law-hearings/news-story/6672d94d340184b9b885e5c1a513fdae>) . *The Courier-Mail*.
38. Prosecutions, Office of the Director of Public (1 August 2024). "Questions of Law Reserved (1 and 2 of 2023)" (<https://www.dpp.sa.gov.au/prosecuting-crimes/cases-of-interest/questions-of-law-reserved-1-and-2-of-20232024sasca-82-27-june-2024>) . *Office of the Director of Public Prosecutions*. Retrieved 19 January 2025.

External links
