# Three major stalkerware apps vanish amid data breach fallout and AWS scrutiny



Three stalkerware applications—Cocospy, Spyic, and Spyzie—have recently vanished, igniting concerns regarding data privacy and security implications in the realm of consumer-grade surveillance tools. These applications, which are known for their ability to covertly monitor individuals, have disappeared from the digital landscape, including their websites and associated cloud storage on Amazon Web Services. The sudden withdrawal of these services has prompted commentary that links their fate to a series of data breaches earlier in the year, although no definitive explanation has yet emerged.

The landscape of spouseware applications is marred by ethical controversies and legal ambiguities. Touted as tools for monitoring minors or individuals with special needs, many such programs operate in a grey area, often facilitating invasive surveillance of partners or family members. The erasure of Cocospy, Spyic, and Spyzie is not unprecedented; similar applications have previously shut down or undergone rebranding in the aftermath of security breaches, attempting to distance themselves from the fallout of compromised user data.

Recent investigations have highlighted alarming vulnerabilities connected to these applications. Cocospy and Spyic, for instance, were revealed to have leaked sensitive data, including email addresses, call logs, and photographs, endangering the privacy of nearly 1.8 million and 880,000 individuals respectively. These breaches have often involved the quiet exfiltration of vast amounts of information, undermining the very privacy these users sought to invade in others.

The menace posed by stalkerware applications has broader implications, suggesting a systemic issue within the software and cloud service industries. A report surfaced regarding a substantial data breach at another stalkerware provider, SpyX, which affected nearly 2 million users and drew attention to the overarching risks involved in deploying such applications. The lack of proactive communication from SpyX regarding the breach has raised critical questions about user awareness and the responsibilities of companies operating in the surveillance domain.

Concerns surrounding the hosting infrastructure for these applications have also come to the forefront, particularly relating to Amazon Web Services. Despite being alerted to the presence of stolen data linked to Cocospy, Spyic, and Spyzie, AWS has faced scrutiny for its apparent inaction in removing this compromised information. Such negligence heightens the question of corporate responsibility in safeguarding sensitive user data, especially when it is being misappropriated within the context of spyware applications.

The issue of stalkerware has garnered increasing attention, with at least 24 monitoring applications having faced significant breaches since 2017. This epidemic of vulnerabilities not only places unwitting victims at risk but also exposes those who employ these applications to the very threats they seek to mitigate. Critics argue that the pervasive use of such tools without proper oversight and regulation creates a legal and ethical quagmire, diminishing the very trust that users place in technology intended for protective or supportive purposes.

As the landscape of personal surveillance continues to evolve, the downfall of these three applications serves as a stark reminder of the potential dangers lurking within that grey zone. The ramifications extend far beyond individual cases, sparking discussions about privacy rights, data integrity, and the need for stringent regulations governing the use of surveillance software. In this rapidly shifting digital age, prioritising user consent and transparency remains paramount to ensuring that technology serves as a tool for empowerment rather than exploitation.

### Reference Map

1. Paragraphs 1, 2, 3, 4, 5, 6
2. Paragraphs 5, 6
3. Paragraphs 3, 4, 5
4. Paragraphs 5, 6
5. Paragraph 4
6. Paragraph 4
7. Paragraph 4

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.techradar.com/pro/security/these-three-stalkerware-apps-have-just-gone-dark-and-a-data-breach-could-be-to-blame> - Please view link - unable to able to access data
2. <https://techcrunch.com/2025/03/19/data-breach-at-stalkerware-spyx-affects-close-to-2-million-including-thousands-of-apple-users/> - A data breach at SpyX, a consumer-grade spyware operation, exposed records of nearly 2 million individuals, including thousands of Apple users. The breach, dating back to June 2024, was not previously reported, and there is no indication that SpyX's operators notified their customers or those targeted by the spyware. The data breach highlights the risks associated with stalkerware applications and their potential to compromise user privacy.
3. <https://www.vpnmentor.com/news/amazon-hosting-stalkerware-victims-data/> - Amazon Web Services (AWS) is under scrutiny for continuing to host stolen data from victims of three stalkerware apps—Cocospy, Spyic, and Spyzie—weeks after being alerted to its presence. These apps, designed for covert surveillance, secretly extract and upload victims' personal data to AWS-hosted storage buckets. Despite being notified in February 2025, Amazon has not taken steps to remove the compromised data, raising concerns about the company's response to data breaches involving its services.
4. <https://techcrunch.com/2025/02/27/hacked-leaked-exposed-why-you-should-stop-using-stalkerware-apps/> - An increasing number of stalkerware companies have experienced significant data breaches, exposing sensitive user information. Since 2017, at least 24 stalkerware companies have been hacked or leaked customer and victims' data online. The article emphasizes the risks associated with using such apps, including potential exposure of personal data and the legal and ethical implications of monitoring individuals without their consent.
5. <https://www.certosoftware.com/insights/stalkerware-app-spyzie-exposes-sensitive-data-of-500k-users/> - The stalkerware app Spyzie has been found to compromise the sensitive data of more than 500,000 Android users and nearly 5,000 iPhone and iPad users. The app shares a critical vulnerability with two other stalkerware apps, Cocospy and Spyic, which recently exposed the personal data of over 2 million people. The security flaw in Spyzie allows unauthorized access to sensitive information, including messages, photos, call logs, and location data collected from infected devices.
6. <https://www.scworld.com/brief/over-500k-android-ios-ipados-devices-impacted-by-spyzie-stalkerware> - More than 500,000 Android devices, as well as at least 4,900 iPhones and iPads, have been unknowingly breached by the Spyzie mobile surveillance app. The app exposed obtained data through the exploitation of a vulnerability recently discovered in the Cocospy and Spyic spyware apps. The flaw allows unauthorized access to pilfered messages, location details, photos, and other phone data, and also exposed 518,643 email addresses belonging to Spyzie customers who sought to infiltrate others' devices.
7. <https://candid.technology/spyzie-data-leak-exposes-half-million-android-devices/> - A surveillance operation called Spyzie has compromised more than 500,000 Android devices and nearly 5,000 iPhones and iPads. The affected owners, mostly unaware of the breach, have had their personal data—including messages, photos, and location—exposed due to a critical security flaw. Spyzie shares the same security vulnerability as Cocospy and Spyic, two other stalkerware applications built on identical source code, allowing unauthorized access to exfiltrated phone data and putting millions of individuals at risk.