# Israeli private investigator faces US extradition over hacking of climate activists



A private investigator from Israel, Amit Forlit, faces extradition to the United States following allegations that he orchestrated a hacking campaign targeting American climate activists. The extradition hearings took place at Westminster Magistrates' Court in London, where a judge recommended that Forlit be sent to the U.S. to face charges brought by the Justice Department.

According to an indictment filed by the U.S. Justice Department, the hacking was commissioned by a Washington, D.C.-based lobbying and consulting firm working on behalf of a major oil and gas company in Texas. The federal allegations assert that the operation aimed to discredit individuals and groups involved in climate-change litigation in the United States. The charges against Forlit include conspiracy to commit computer hacking, conspiracy to commit wire fraud, and wire fraud. Forlit has denied any involvement in ordering or paying for the hacking.

Forlit’s lawyer, Edward Grange, told reporters outside the London court that the ruling marked the start of a “long road” ahead, adding, “The score is one-nil to the U.S.” Forlit has two weeks to appeal the decision.

Victims of the hacking, comprising climate and environmental activists, view the attacks as an attempt to silence opponents of the fossil fuel industry. Lee Wasserman, director of the Rockefeller Family Fund and a hacking target, highlighted the wider implications of the case, stating, “It’s a very big issue that transcends, really, the most basic aspects of freedom and citizens’ ability to participate in their governmental processes.” Kathy Mulvey, climate accountability campaign director at the Union of Concerned Scientists, also underscored the significance of the extradition proceedings in shedding light on the responsible parties and establishing accountability.

The indictment and accompanying affidavit include allegations linking the hacking campaign to a lobbying firm referenced in part as the “D.C. lobbying firm.” The affidavit reveals emails showing the sharing of stolen documents, including a memo belonging to an environmental lawyer, between employees of this firm. The firm identified in this context is DCI Group, which has longstanding ties to ExxonMobil and the fossil fuel sector. A court filing by Forlit’s legal team earlier this year stated that the hacking was “alleged to have been commissioned by DCI Group, a lobbying firm representing ExxonMobil, one of the world’s largest fossil fuel companies.”

Craig Stevens, a DCI executive, denied the allegations, calling them "false and unsubstantiated," and emphasised that the company directs all its employees and consultants to comply with the law. ExxonMobil similarly distanced itself from the hacking accusations, stating it has not been involved in or aware of such activities and condemns any hacking in the strongest terms.

This case is situated within a broader context where fossil fuel companies, including ExxonMobil, face numerous lawsuits from states and municipalities accusing them of misleading the public about the dangers of fossil fuel emissions and climate change. These legal actions seek compensation to help communities deal with climate-related damages such as extreme weather events. The companies, however, describe these lawsuits as politically motivated and insist that climate policy should be handled by Congress rather than the courts.

The investigation into the hacking was further marked by the sentencing of Aviram Azari, another Israeli private investigator associated with Forlit. Azari pleaded guilty to conspiracy to commit computer hacking, wire fraud, and aggravated identity theft, having hired hackers to target American climate activists, government officials in Africa, members of a Mexican political party, and critics of a German company. Prosecutors noted that ExxonMobil had used news stories based on stolen information to defend itself against state investigations but did not accuse the company or DCI of wrongdoing in Azari’s case.

Forlit was arrested at London’s Heathrow airport months after Azari’s sentencing, following an Interpol Red Notice. The Justice Department’s affidavit details a scheme whereby the lobbying firm identified targets to discredit, then allegedly passed lists of people or accounts to Forlit or his associates. Azari then engaged hackers to carry out the attacks on these climate activists. Stolen documents obtained through these hacks were shared with the oil company and subsequently appeared in media reports aimed at undermining the credibility of civil investigations against the company. The oil company allegedly relied on these media reports in court filings to contest the climate litigation.

The Oregon Public Broadcasting (OPB) is reporting on the developments of this case, which remains ongoing as Forlit’s legal team prepares for potential appeals following the extradition recommendation.

This extensive case highlights the interplay between climate activism, corporate lobbying, and cybersecurity, with significant implications for legal and political dynamics surrounding climate change accountability and industry practices.

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

## Bibliography

1. <https://www.reuters.com/world/israeli-private-eye-wanted-us-over-alleged-hacking-exxon-lobbyist-lawyer-says-2025-01-22/> - This article reports on the extradition proceedings of Israeli private investigator Amit Forlit, who is accused by the U.S. of orchestrating a hacking campaign targeting American climate activists. The U.S. alleges that Forlit was commissioned by a Washington, D.C.-based lobbying firm representing a major oil and gas company to discredit individuals involved in climate-change litigation.
2. <https://www.reuters.com/business/energy/us-senators-green-groups-call-accountability-over-hacking-exxon-critics-2024-12-12/> - This piece discusses the reactions of U.S. senators and environmental groups to the hacking campaign targeting ExxonMobil critics. It highlights calls for investigations and accountability, with the FBI reportedly investigating DCI Group, a lobbying firm associated with ExxonMobil, over its potential involvement in the hacks.
3. <https://www.npr.org/2025/01/24/nx-s1-5271530/hacking-investigation-climate-change> - This NPR article details the U.S. investigation into a hacking campaign that targeted climate activists. It mentions that the hacking was allegedly commissioned by a Washington, D.C.-based lobbying firm working on behalf of a major oil and gas company, aiming to discredit individuals involved in climate-change litigation.
4. <https://www.ucs.org/about/news/exxonmobil-lobbyist-dci-cyberattack-investigation> - This report from the Union of Concerned Scientists discusses the FBI's investigation into DCI Group, a longtime ExxonMobil lobbying firm, for its potential involvement in a cyberattack targeting climate accountability advocates. The article notes that ExxonMobil has not been publicly implicated in the illegal hacking operation.
5. <https://www.npr.org/2025/01/24/nx-s1-5271530/hacking-investigation-climate-change> - This article provides an overview of the U.S. investigation into a hacking campaign that targeted climate activists. It mentions that the U.S. is trying to extradite Israeli private investigator Amit Forlit, who is accused of orchestrating the hacking campaign commissioned by a lobbying firm representing a major oil and gas company.
6. <https://www.reuters.com/business/energy/us-senators-green-groups-call-accountability-over-hacking-exxon-critics-2024-12-12/> - This piece discusses the reactions of U.S. senators and environmental groups to the hacking campaign targeting ExxonMobil critics. It highlights calls for investigations and accountability, with the FBI reportedly investigating DCI Group, a lobbying firm associated with ExxonMobil, over its potential involvement in the hacks.
7. <https://news.google.com/rss/articles/CBMiqAFBVV95cUxPZ2prZjNRQ2EtMlFuam9uX1ZiTWxLcmM1ajFkWHhxZ2RDRlFSekhWdGczcXZJTGwwUlczdHdocGRCaXdrWmN1U1R0QlRRRlhfTl84aDhwQjVDYXFkR1dJSTZUMHdFMUFpMlhCR3VrbEFpMl9hWC1LcHZwVG1BYjdDTF9GaXI1SktuYkhrNkJWRGtqRVVWRlRTY0VBSEs0OVgtNzFfWUpBWnI?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data