

CIA Adapts Database Software Called PROMIS with Back Door for Cyber-espionage

By [Dr. Jack Colhoun](#)

Global Research, September 27, 2022

[CovertAction Magazine](#) 23 February 2021

Region: [USA](#)

Theme: [Intelligence](#)

All Global Research articles can be read in 51 languages by activating the “Translate Website” drop down menu on the top banner of our home page (Desktop version).

To receive Global Research’s Daily Newsletter (selected articles), [click here](#).

Follow us on [Instagram](#) and [Twitter](#) and subscribe to our [Telegram Channel](#). Feel free to repost and share widely Global Research articles.

Did the CIA lie, cheat and betray its friends and business partners in ways that even Donald Trump might envy? A rapidly unfolding intelligence scandal indicates that the answer is yes.

The dark world of cyber-age espionage is on full display in the unfolding scandal involving the CIA and Crypto AG, the encryption company based in Zug, Switzerland.

Washington Post investigative reporter Greg Miller, drawing on a 96-page CIA report, [disclosed that Crypto AG had been secretly purchased in June 1970 by the CIA and the BND, the then West German foreign intelligence service, for \\$5.75 million.](#)

The BND sold its share in Crypto to the CIA in 1993. Crypto AG, which also collaborated closely with the National Security Agency, was liquidated in 2018.^[1]

Crypto AG sold encryption machines to more than 100 governments seeking protection for diplomatic communications and other sensitive records.

[Miller explained to National Public Radio’s “Fresh Air”](#) that encryption machines

scramble messages and code them and then decode them at the other end so that governments can’t listen to what you’re saying to your diplomats or to your military or to your spies. It’s designed to protect the secrecy of countries communications.

Little did Crypto AG’s customers know that the encryption company they hired to safeguard their sensitive records secretly downloaded them to the CIA and BND.

The CIA history of the Crypto operation called it “the intelligence coup” of the 20th century. The [Agency boasted](#),

foreign governments were paying good money to the U.S. and West Germany to have

their most secret communications read by at least two...foreign countries.

According to the CIA history, "Crypto machines supplied roughly 40 percent of all the foreign communications U.S. code breakers processed for intelligence."^[2]

As the Crypto AG scandal unfolded, Swiss public broadcaster SRF revealed that Omnisec, a second Swiss encryption company, also shared the secrets of its government clients with the CIA and the BND.

[SRF reported](#) that, "like Crypto, Omnisec had sold manipulated equipment to foreign governments and armies."

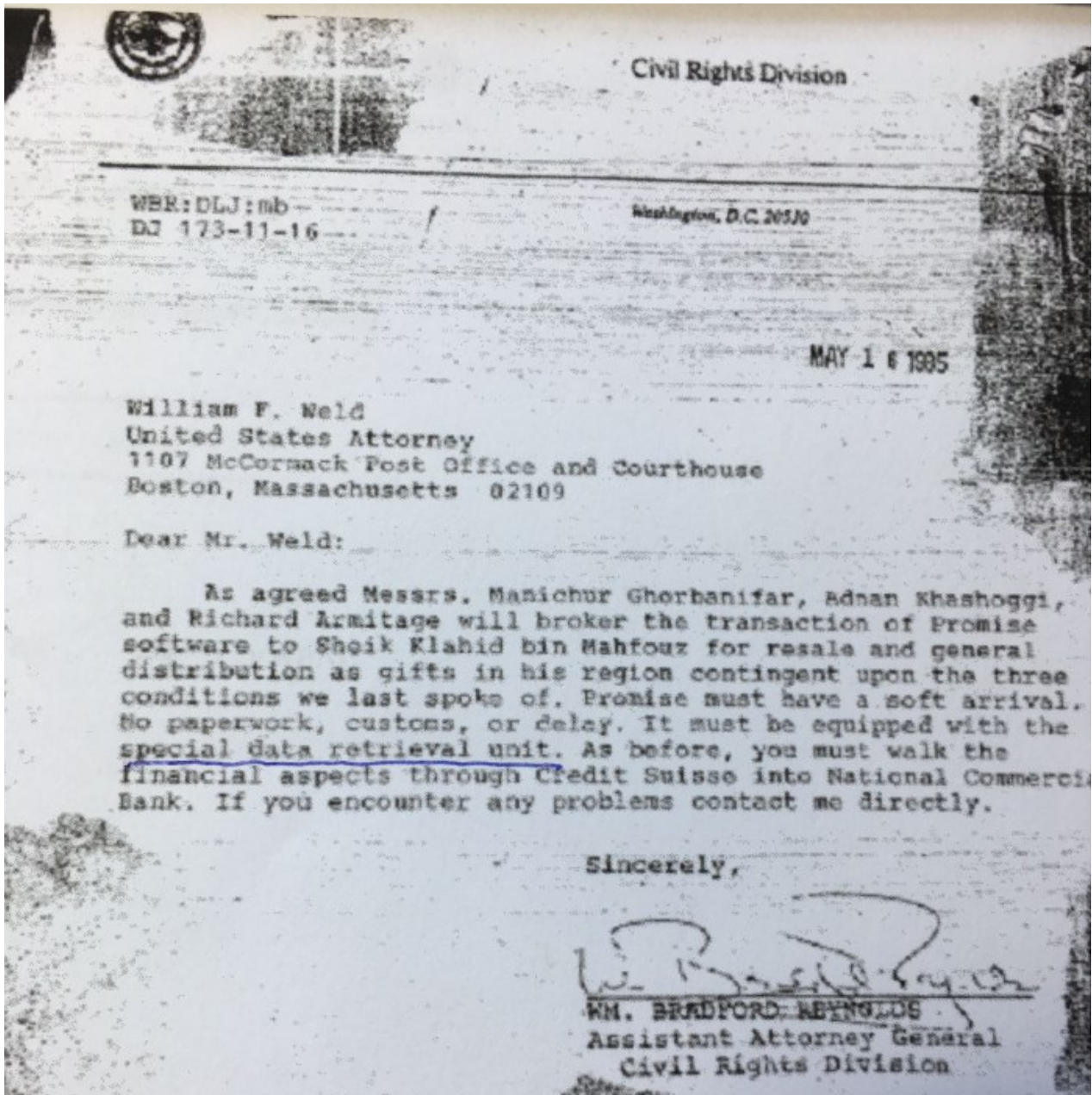
SRF added, "An investigation by the Swiss Parliament...concluded...that Switzerland's own intelligence service had benefitted from the information gathered by its foreign counterparts through the encryption firm." Omnisec, one of Crypto AG's biggest competitors, also sold "manipulated" encryption devices to UBS, Switzerland's largest bank.^[3]

Meanwhile, *CovertAction Magazine* has obtained new evidence in the PROMIS software affair, a related cyber-espionage scandal during the Reagan administration.

The new evidence involves a secret U.S. plan to distribute PROMIS databases, with "a back door," to collect intelligence in the Middle East in the mid-1980s.

Modified copies of the database enabled the CIA to download the secrets countries stored on PROMIS.

A letter dated May 14, 1985, from Assistant Attorney General William Bradford Reynolds to U.S. Attorney William F. Weld in Boston, outlines a covert plan to distribute PROMIS databases with "a special retrieval unit" in the Middle East.



Letter from Assistant Attorney General William Bradford Reynolds to U.S. Attorney William F. Weld in Boston, outlining covert plan to distribute adapted PROMIS databases with "a special retrieval unit" [read: back door] for use in secret U.S. intelligence operations. [Source: Jack Colhoun]

Reynolds wrote,

"As agreed, Messrs. Manucher Ghorbanifar, Adnan Khashoggi, and [Assistant Secretary for Defense] Richard Armitage will broker the transaction of Promise [*sic*] software to Sheik Khalid bin Mahfouz for resales and general distribution or as gifts on his region."

Reynolds insisted,

"Promise [*sic*] must have a soft arrival. No paper work, customs, or delay." He added importantly, "It must be equipped with the special retrieval unit. As before, you must walk the financial experts through the Credit Suisse into National Commerce Bank."^[4]

Ghorbanifar, an Iranian, and Khashoggi, a Saudi, were arms dealers. Mahfouz, a Saudi

financier, represented the National Commerce Bank.^[5]

Unlike Crypto AG or Omnisec, Inslaw, Inc., which developed PROMIS software in the early 1980s, was not owned by the CIA and the BND. Inslaw, which was privately owned, claimed that senior officials in the Reagan administration conspired with the Department of Justice to acquire PROMIS illegally by driving the company into bankruptcy. Inslaw also asserted that modified PROMIS was used in secret U.S. intelligence operations.

“The Inslaw Affair,” a September 1992 investigative report by the House Judiciary Committee, found the small Washington, D. C., software firm’s claims credible.

The Judiciary Committee report stated,

“There appears to be strong evidence, as indicated by the findings in two Federal court proceedings as well as by the committee investigation, that the Department of Justice ‘acted willfully and fraudulently’ and ‘took, converted and stole’ Inslaw’s Enhanced PROMIS by ‘trickery, fraud and deceit.’” Further, the report stated, “It appears that these actions against Inslaw were implemented...under the direction of high-level Justice Department officials.”^[6]

There has not been a full official accounting of the PROMIS affair. But the May 1985 letter from Assistant Attorney General Reynolds to U.S. Attorney Weld on PROMIS is a good place to start.

*

Note to readers: Please click the share buttons above or below. Follow us on Instagram and Twitter and subscribe to our Telegram Channel. Feel free to repost and share widely Global Research articles.

Jack Colhoun is an independent historian of the Cold War (University of Wisconsin, Madison, BA, 1968; York University , PhD, 1976), an investigative reporter and professional archival researcher. Colhoun has written widely on U.S. foreign policy and covert intelligence operations. His work has appeared in the Washington Post, Toronto Star, The Nation, The Progressive, National Catholic Reporter, Covert Action Quarterly and CovertAction Magazine. Colhoun can be reached at: JHColhoun@aol.com.

Notes

[1] Greg Miller, “The Intelligence Coup of the Century,” *Washington Post*, February 20, 2020; Greg Miller interview, “Fresh Air,” National Public Radio, March 20, 2020; for background on Crypto AG, see Wayne Madsen, “Crypto AG: The NSA’s Trojan Whore?” *CovertAction Magazine*, Winter 1998.

[2] Greg Miller interview, National Public Radio, March 20, 2020; Greg Miller, “Swiss Report: CIA’s Ownership of Crypto Jeopardized Neutrality,” *Washington Post*, November 11, 2020.

[3] “Report Claims CIA Controlled Second Swiss Encryption Firm,” *Agence France-Presse*, November 27, 2020; “Second Swiss Firm Allegedly Sold Corrupted Encryption Spying Devices,” Swiss Public Television SWI, November 26, 2020.

[4] Letter from Assistant Attorney General William Bradford Reynolds to U.S. Attorney William F. Weld,

Boston, May 14, 1985.

[5] Peter Truell and Larry Gurwin, *False Profits: The Inside Story of BCCI, the World's Most Corrupt Financial Empire* (Boston: Houghton Mifflin, 1992), 37, 134-36; Jonathan Beaty and S. C. Gwynne, *The Outlaw Bank: A Wild Ride into the Secret Heart of BCCI* (New York: Random House, 1993), 172, 328, 348, 352.

[6] "The Inslaw Affair," An Investigative Report of the House Judiciary Committee, September 10, 1992, 4-6.

Featured image is from muckrock.com

The original source of this article is [CovertAction Magazine](#)
Copyright © [Dr. Jack Colhoun](#), [CovertAction Magazine](#), 2022

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Dr. Jack Colhoun](#)

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca
www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca