

US district court judge orders shutdown of whistleblower web site

Dan Conway
28 February 2008

In an extraordinary act of censorship, lawyers representing the Swiss bank Julius Baer (BJB) obtained an injunction against the Dynadot corporation, US domain name registrar for the Wikileaks web site.

Judge Jeffrey White of the Federal District Court in San Francisco issued the injunction February 15 in a lawsuit BJB filed against Wikileaks and Dynadot. The suit was filed after Wikileaks posted documents allegedly revealing fraudulent activities, including asset-hiding, money laundering and tax evasion schemes, on the part of the bank's Cayman Islands branch. BJB claims the documents were stolen and contain customer information protected from disclosure under privacy laws.

The website of BJB promotes the bank as "the leading dedicated wealth manager in Switzerland," concentrating on "private banking and asset management for private and institutional clients."

Under the terms of the injunction, Dynadot may not release the registered wikileaks.org domain name, meaning that the Wikileaks web site cannot be reached through the related web address, www.wikileaks.org. Various overseas mirror, or duplicate, sites remain operational. (For a list of such addresses, click here http://en.wikipedia.org/wiki/Wikileaks#External_links).

A domain name registrar, such as Dynadot, is a company that typically has been accredited by ICANN, the Internet Corporation for Assigned Names and Numbers, to register domain names. Many such companies, including Dynadot, also act as DNS (Domain Name System) hosting services.

DNS hosting services are used to translate a given domain or host name—the human readable name of a device connected to the internet such as a web server—into its associated numerical IP address, which then allows access to the associated web site. The injunction against Dynadot effectively prevents this from occurring in the case of Wikileaks.

The judge's ruling ordered Dynadot to "immediately clear and remove all hosting records for the wikileaks.org domain name and prevent the domain name from resolving to the wikileaks.org web site or any other web site or server other than a blank park page, until further order of this Court."

The Wikileaks website began posting material in December 2006 with the stated goal of allowing corporate and government whistleblowers to anonymously release sensitive documents onto the Internet without fear of retribution. The site now says it is in possession of over 1.2 million such documents and was responsible for publicizing:

- * The US Military's "Rules of Engagements for Iraq," which outline authorization protocols for engaging in missions that anticipate collateral damage;

- * Documents showing alleged money laundering activities on the part of former Kenyan president Daniel Arap Moi;

- * The 238-page "Standard Operating Procedures for Camp Delta," which, among other procedures, authorizes disciplinary action against detainees who damage "government-issued styrofoam cups";

- * A 2007 sales document sent by Britain's Northern Rock to potential bidders which reported that the struggling bank could still owe £6 billion of an original £24 billion to the Bank of England in 2010.

There have been several additional attacks on Wikileaks in recent weeks. The website's servers in Sweden suffered a 500 megabyte-per-second "distributed denial of

service” (DDoS) attack shortly after the February 15 injunction, followed by an actual server fire.

A denial of service attack typically entails the sending of multiple false communication requests to a web server so that the server is no longer able to respond to legitimate external requests. A DDoS is a more advanced version, involving the use of multiple systems to target the web server. The chances that such an attack could trigger an actual fire are slight, especially with up-to-date safety mechanisms in place. It is still unclear who was behind the DDoS and what caused the fire.

The February 15 injunction is by no means the first attempt to suppress content on Wikileaks. Lawyers for Northern Rock attempted, unsuccessfully, to remove its 2007 sales document from the site.

Unlike the Northern Rock case, however, lawyers for BJB took the extra step of seeking to enjoin the domain name, effectively silencing wikileaks.org. Many online commentators have drawn the counterfactual historical analogy of the Nixon Administration shutting down the entire *New York Times* for publishing the Pentagon Papers in 1971, instead of its actual response—a suit to impose a court injunction against the *Times* to stop publication of excerpts from the papers.

Judge Jeffrey White, a 2002 Bush appointee, had previously sentenced two *San Francisco Chronicle* reporters to 18 months in prison after they refused to reveal their sources for articles written about the performance-enhancement drug scandal in professional baseball. The articles had used leaked grand jury testimony by Barry Bonds and other players that implicated a Bay Area nutritional supplement company in the operations of a clandestine steroid distribution ring.

White’s ruling also requires Dynadot to remove privacy constraints in relation to the wikileaks.org domain name to allow the gathering of Wikileaks’ administrative contact information.

In addition to the injunction against Dynadot, Judge White issued a temporary restraining order against Wikileaks, which orders Wikileaks to cease posting any BJB-related documents and to return them. In this case, Wikileaks did not obtain legal counsel to appear and contest the temporary order.

A second hearing has been scheduled for February 29, at which time Judge White will decide whether to convert the temporary restraining order against Wikileaks into a preliminary injunction, one that lasts during the period of the lawsuit. So far Wikileaks has not obtained counsel to file papers opposing the injunction, so it is likely the court

will issue it on the 29th.

The documents in question purportedly include files that had been sent to US tax authorities as far back as 2002. Despite BJB’s claims that the documents had been stolen from its Grand Cayman office, the bank never filed a formal complaint with the Royal Cayman Islands Police Service. Instead the bank hired private investigators to search the homes of its branch employees and later required them to take polygraph tests once the searches had proven fruitless.

One of the employees tested was Rudolf Elmer, former chief operations officer for the Cayman branch. The bank apparently concluded that Elmer was behind the leaks after the polygraph results came in. Elmer had been preparing for spinal surgery at the time, and later complained to the American Polygraph Association, one of whose agents conducted the test. The association informed him that rules of conduct for “ethical polygraphing” did not apply to the Cayman Islands.

Elmer claims that he then received anonymous phone calls that advised him and his family to return to Switzerland “for their own good.”

The bank subsequently terminated Elmer’s employment, at which point he and his family returned to Zurich. Elmer alleged in a legal application to the prosecutor’s office in Zurich-Sihl that he and his family continued to receive frequent harassing phone calls upon their return. The prosecutor’s office denied Elmer’s application.

The bank itself believes that Elmer was the source of the leaks, which he himself denies, while claiming possession of sensitive BJB documents to insure his family’s safety.

The Cayman Islands, located in the Caribbean Sea approximately 180 miles south of Cuba, have long been considered a haven for the ultra-rich and politically well-connected to launder money and evade taxes.



To contact the WSWS and the Socialist Equality Party visit:

wsws.org/contact