NEWS

The U.S. Government Has Amassed Terabytes of Internal WikiLeaks Data

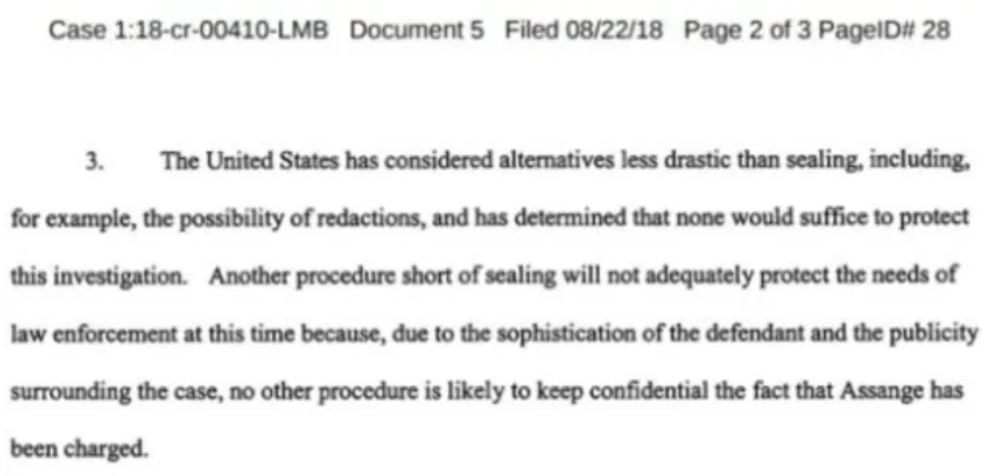
Emma Best
Today 9:00am •

14.7K 20 2

Photo: Frank Augstein (AP)

Late last year, the U.S. government accidentally revealed that a sealed complaint had been filed against Julian Assange, the founder of WikiLeaks. Shortly before this was made public, the FBI reconfirmed its investigation of WikiLeaks was ongoing, and the Wall Street Journal reported that the Department of Justice was optimistic that it would be able to extradite Assange. Soon after, portions of sealed transcripts leaked that implicate WikiLeaks and Assange in directing hackers to target governments and corporations. The charges against Assange have not been officially revealed, though it's plausible that the offenses are related to Russian hacking and the DNC emails.

The alleged offenses in the complaint notwithstanding, the government has an abundance of data to work with: over a dozen WikiLeaks' computers, hard drives, and email accounts, including those of the organization's current and former editors-in-chief, along with messages exchanged with alleged Russian hackers about DNC emails. Through a series of search warrants, subpoenas, equipment seizures, and cooperating witnesses, the federal government has collected internal WikiLeaks data covering the majority of the organization's period of operations, from 2009 at least through 2017.



Case 1:18-cr-00410-LMB Document 5 Filed 08/22/18 Page 2 of 3 PageID# 28

3. The United States has considered alternatives less drastic than sealing, including, for example, the possibility of redactions, and has determined that none would suffice to protect this investigation. Another procedure short of sealing will not adequately protect the needs of law enforcement at this time because, due to the sophistication of the defendant and the publicity surrounding the case, no other procedure is likely to keep confidential the fact that Assange has been charged.

The filing that committed a copy and paste error revealing charges against Assange.

In some instances, the seized data has been returned and allegedly destroyed, such as in the case of David House, a technologist and friend of Chelsea Manning when she famously became a source for WikiLeaks. In others, the seized materials include communications between WikiLeaks and their sources. Some of these discussions show WikiLeaks discussing their other sources and specific identifying details about them.

A copy of a chat log between Chelsea Manning and a WikiLeaks staff member IDed as Assange by government prosecutors and witnesses.

Other seizures gave authorities a deeper view of the internal workings of WikiLeaks, including one of the earliest known seizures of WikiLeaks-related data, executed on December 14, 2010, when the messages and user information of several WikiLeaks-linked Twitter accounts were ordered. This search-and-seizure order included direct messages associated with WikiLeaks and its founder, former Army private first class and WikiLeaks source Chelsea Manning, WikiLeaks editor Rop Gongrijp, former WikiLeaks associate Jacob Appelbaum, and former WikiLeaks associate and Icelandic MP Birgitta Jonsdottir, between November 1, 2009, and the order's execution.

A couet order for information relating to people associated with WikiLeaks.

On January 4, 2011, a sealed order filed in the Eastern District of Virginia requested all emails, address book, subscriber information, and other account information associated with Appelbaum's email address

ioerror@gmail.com, and another order would target his internet traffic. Appelbaum was a friend and confidant of Assange as well as a WikiLeaks volunteer. In 2010, Appelbaum was known as "the American WikiLeaks hacker," and he was, at that time, referred to as WikiLeaks' only known American member. In a private chat in 2015, WikiLeaks described Appelbaum as being "sort of" part of the group, though following multiple accusations of sexual abuse, the group publicly distanced itself from him. The emails obtained by the government extended from November 2010 at least through January 2011. The timing of the government's acknowledgment of the order, along with other similar orders, suggest that the monitoring of the account may have continued through late 2014, when it and several orders were made public.

A copy of a court order for information relating to Jacob Appelbaum, a hacker who worked with WikiLeaks (now credibly accused of multiple sexual assaults).

Publicly released and leaked documents from Assange and his legal team allege that several laptops and hard drives belonging to the organization were intercepted by an intelligence agency during this time period. According to an affidavit from Assange, "three laptops ... assorted

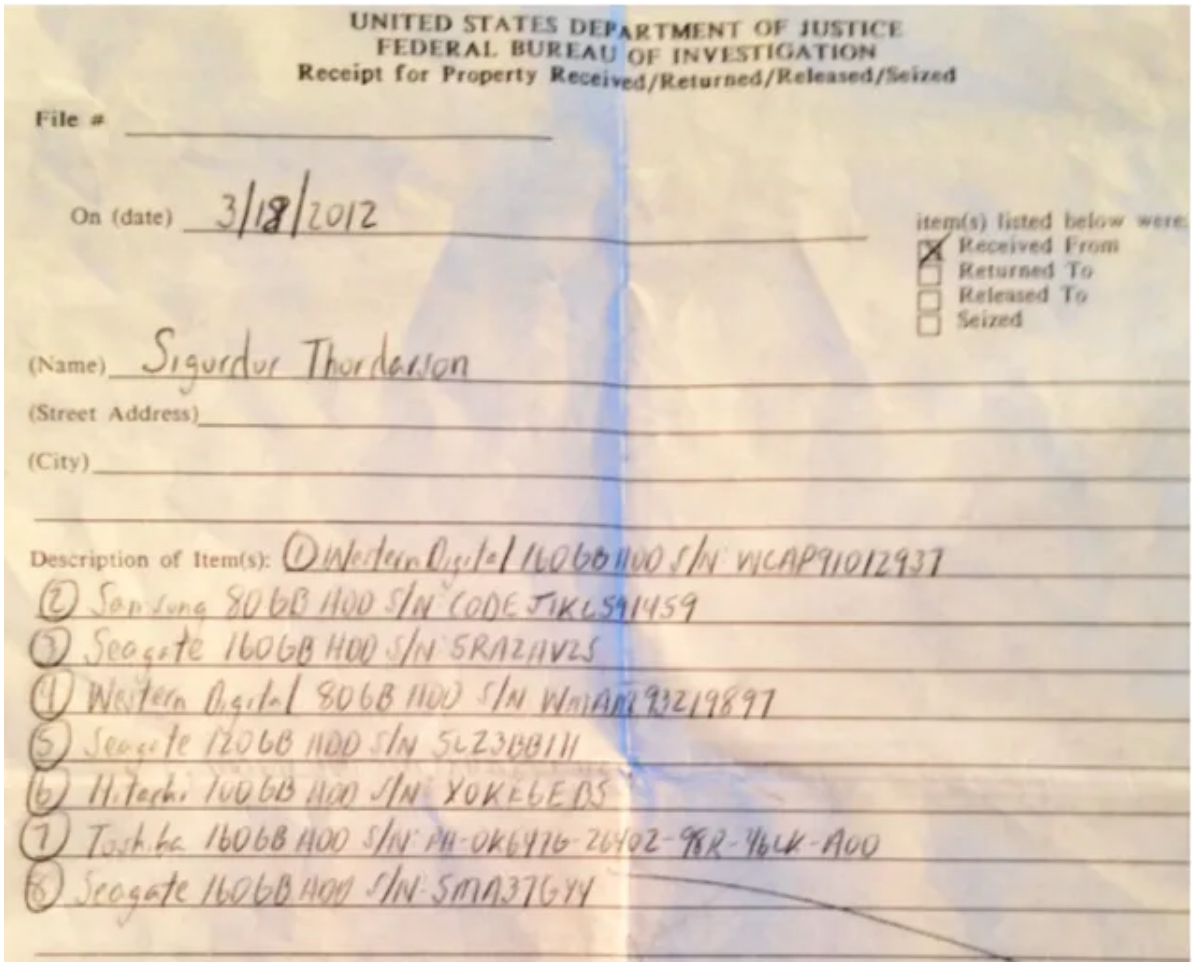
electronics [and] additional encrypted hard drives" were taken along with his suitcase in late September 2010. Assange's legal team produced several additional affidavits and supporting documents detailing the existence and disappearance of the suitcase. The suitcase contained at least five hard drives, all of which were encrypted, according to Assange. However, the government has had eight years to guess or recover the passwords or break the encryption on the hard drives. Several other drives, numerous emails, and at least one cooperating witness may have aided in the process.

Affadavit from Julian Assange.

In mid-2011, the FBI had developed a major source who would become at least their second information with an eye into WikiLeaks' operations. Soon after the arrest and cooperation of Hector Xavier Monsegur, a.k.a. Sabu, his hacking group (LulzSec) made contact with WikiLeaks. Sabu and LulzSec would become some of WikiLeaks' most significant sources. The Syria files and Global Intelligence files LulzSec provided WikiLeaks increased their number of publications tenfold and still account for roughly half of their total number of publications. Communications between Sabu and WikiLeaks were monitored by the FBI. And some of the group's communications with others were later seized in their arrest or turned over by Sigurdur Thordarson, a WikiLeaks volunteer who became an informant for the FBI that August.

A section from the sentencing document for "Sabu." It was later ID'd by WikiLeaks as about them.

In addition to briefing the FBI in a series of meetings, Thordarson reportedly provided them with thousands of pages of WikiLeaks chat logs. Further, in March 2012, Thordarson allegedly provided the FBI with eight WikiLeaks hard drives containing up to 1020GB of data, according to a purported FBI document. Officials have not confirmed the authenticity of the document, though the amount of data provided is corroborated by additional sources. In an interview with *Ars Technica*, Thordarson claimed that Icelandic authorities had seized an additional 2 TB of WikiLeaks-related data from him, which he assumed was then shared with the U.S. American and Icelandic authorities had previously cooperated on Thordarson's case and portions of the WikiLeaks investigation. According to leaked letters from WikiLeaks' legal team, at least some of the hard drives had belonged to Assange. Thordarson's debriefings and the hard drives of up to 3 TB of data may have contained the decryption keys or passwords needed to decrypt the hard drives Assange alleged had been seized earlier.



UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # _____

On (date) 3/18/2012

item(s) listed below were:
☒ Received From
☐ Returned To
☐ Released To
☐ Seized

(Name) Sigurdur Thordarson

(Street Address) _____

(City) _____

Description of Item(s):
① Western Digital 1606B HDD S/N WCAP91012937
② Samsung 80GB HDD S/N CODE JIKL591459
③ Seagate 160GB HDD S/N 5RA2HV2S
④ Western Digital 80GB HDD S/N WMAM9219897
⑤ Seagate 120GB HDD S/N 5LZ3BB1H
⑥ Hitachi 160GB HDD S/N YOKEGEDS
⑦ Toshiba 160GB HDD S/N MK6416 26402-9KR-96LK-A00
⑧ Seagate 160GB HDD S/N 5MA37GYY

A receipt given to Sigurdur Thordarson from the FBI for WikiLeaks hard drives.

There are several hints as to the contents of these drives. According to the affidavit from Assange, the information on the hard drives included, in addition to the possible staff emails, "chat communications ... copies of passports [and] video footage taken in secret." Following an Associated Press article based off of a cache of "WikiLeaks emails, chat logs, financial records, secretly recorded footage and other documents" from within the organization, WikiLeaks alleged that the cache was the same that had been provided to the FBI.

In October 2011, amidst Thordarson and Sabu's tenure as cooperating witnesses, American authorities issued a search warrant for the contents of WikiLeaks volunteer Herbert Snorrason's Gmail account. The warrant requested all of the account's information, "including stored or preserved copies of e-mails sent to and from the account, draft e-mails, deleted e-mails, emails preserved pursuant to a request made under 18 U.S.C. § 2703(f), the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail." The volunteer had helped WikiLeaks with a minor technical issue. After learning that his account's contents had been seized by the U.S. government, Snorrason told Mother Jones that he thought "pretty much everyone with both a Google account and a WikiLeaks connection will be getting one of those notices eventually." Snorrason was correct in that other WikiLeaks-associated Google accounts had their information seized by the government.

Six months after the order for Snorrason's emails was issued, a trio of search orders were issued for the email accounts of senior WikiLeaks personnel. On April 5, 2012, sealed warrants were executed for the Google accounts of WikiLeaks editors Sarah Harrison and Joseph Farrell, as well as then-spokesman and future editor-in-chief Kristinn Hrafnsson on suspicion of espionage and violating the Computer Fraud and Abuse Act, as well as conspiracy and theft of government property. The warrants appear to have covered the entirety of the accounts and were disclosed by Google at the close of 2014.

A court order for information relating to Kristinn Hrafnsson, current editor in chief of WikiLeaks, on suspicion if charges including but not limited to espionage.

In late October 2017, a new government request was issued for portions of WikiLeaks' communications. A letter from Sen. Diane Feinstein requested that Twitter provide copies of all direct messages that were over 180 days to or from the accounts belonging to WikiLeaks, the WikiLeaks Task Force, "Guccifer 2.0," Assange, and Margaret Ratner Kunstler. As written, the request would include some of my communications with WikiLeaks and "Guccifer 2.0." Ultimately, at least some messages between WikiLeaks and the "Guccifer 2.0" were obtained by the U.S. government, although the method of communication for those messages remains unconfirmed.

According to what's informally known as "the GRU indictment," WikiLeaks sent Guccifer 2.0 a message on June 22, 2016. The message instructed Guccifer 2.0, a persona the U.S. government believes was used by Russian operatives, to send new material to them so it would "have a

much higher impact." On approximately July 6, the organization sent another message encouraging Guccifer 2.0 to send "anything [H]illary related" in time for the Democratic National Convention, which WikiLeaks thought Clinton would use to solidify support. The quoted portion of the exchange ends with WikiLeaks saying they thought conflict between Sen. Bernie Sanders and Clinton would be "interesting." These exchanges, about maximizing impact and damage, are relevant to one of the theories of Assange's potential prosecution outlined by noted national security journalist Marcy Wheeler.

a. On or about June 22, 2016, Organization 1 sent a private message to Guccifer 2.0 to "[s]end any new material [stolen from the DNC] here for us to review and it will have a much higher impact than what you are doing." On or about July 6, 2016, Organization 1 added, "if you have anything hillary related we want it in the next tweo [*sic*] days prefable [*sic*] because the DNC [Democratic National Convention] is approaching and she will solidify bernie supporters behind her after." The Conspirators responded, "ok . . . i see." Organization 1 explained, "we think trump has only a 25% chance of winning against hillary . . . so conflict between bernie and hillary is interesting."

An excerpt from a Mueller indictment.

If the charges against Assange are related to Russian hacking and the Democratic National Committee email leak, this exchange could be one of the most likely pieces of evidence to be directly relevant to the initial charges against him. However, the entirety of the government's evidence, including materials seized from alleged Vault 7 leaker Joshua Schulte and the alleged recordings of him transferring additional files to WikiLeaks regarding the organization, may be used to help make the case. Past statements and communications may be used to help establish a *modus operandi*, a pattern or an intent. As noted by the AP, some of the materials may point to the early beginnings of Assange's reported relationship with Russia. Leaked copies of sealed files, statements by people familiar with the grand juries, and documents released through FOIA by independent journalist Alexa O'Brien—who also identified a number of sealed search orders—all indicate that the investigations converged and pooled

evidence at times. The government's information could be further augmented by recent surveillance of Assange in the Ecuadorian Embassy, where he has lived under asylum since 2012, the fruits of which may have reportedly been shared with the United States.

Regardless of what the charges against Assange are, the government has terabytes of data with which to try to make its case, data that's come from WikiLeaks supporters, sources, key personnel, and Assange himself. The full depth of the government's sources, however, have yet to be revealed.

Emma Best is a national security reporter and transparency activist. She has published millions of pages of government documents and is a member of the leak collective Distributed Denial of Secrets (DDoSecrets).

ABOUT THE AUTHOR

Emma Best

Emma Best

Emma is a national security reporter and transparency activist. She has published millions of pages of government documents, and is a member of the leak collective Distributed Denial of Secrets.

Twitter Posts