{* LEGAL *}

Archive.org's Wayback Machine is legit legal evidence, US appeals court judges rule

Big thumbs up to Internet Archive for now

Kieren McCarthy in San Francisco
Tue 4 Sep 2018 // 19:38 UTC

61

ANALYSIS The Wayback Machine's archive of webpages is legitimate evidence that may be used in litigation, a US appeals court has decided.

The second circuit ruling [PDF] supports a similar one from the third circuit – and, taken together, the decisions could pave the way for the Internet Archive's library of webpages to be considered evidence for countless future trials.

The second circuit, based in New York, was asked over the summer to review an appeal by an Italian computer hacker in which he sought to exclude screenshots of websites run by him that tied him to a virus and botnet he was ultimately convicted over. Prosecutors had taken screenshots of his webpages from the Internet Archive and used them as trial evidence – and he wanted the files thrown out.

Fabio Gasperini argued that the presented Wayback Machine archives of his webpages were not adequately authenticated as legit and untampered, and so shouldn't have been included in his criminal trial. He cited a decision by the second circuit to argue his point, noting that in a 2009 case, the appeals court had agreed with a lower district court decision to exclude screenshots of Wayback Machine snapshots because their authenticity could not be proven.

However, the second circuit argued that its decision in that earlier case was over whether the district court had made an error in excluding the screenshots of the archived pages, and it decided only that the court had followed its rules and so had not made an error. In other words, it didn't make a determination over the validity of the snapshots themselves, only whether the process had been followed.

In the Gasperini case, however, the second circuit noted that the prosecution had included testimony from the Internet Archive's office manager, "who explained how the Archive captures and preserves evidence of the contents of the internet at a given time."

The Wayback Machine works by crawling over the web with bots that automatically fetch as many pages as they can find and store it all in a searchable public database, effectively snapshotting the world's websites on a given day. For instance, if you want to see what *The Register* looked like in 1998, go right ahead.

The manager also testified that the prosecution's screenshots of the Wayback Machine's archive of Gasperini's webpages really did match the contents of the Internet Archive. And, combined, this created a sufficient degree of

authenticity. Gasperini's lawyers were also able to cross-examine the office manager, the appeals court noted.

Take two

The appeals judges' decision reflected a similar one back in 2011 by the third circuit (United States v. Bansal) where a witness testified "from personal knowledge" how the Wayback Machine worked and how reliable it was. The court decided this provided "sufficient proof" that its mirrored pages were authentic.

Taken together, this latest decision gives a strong foundation for the Wayback Machine to be seen as a legit source of future evidence – something that is likely to become ever more important as the internet continues to pervade all aspects of our lives.

Of course, it may still be the case that if a prosecution does not have an Internet Archive staffer to act as a witness in a case to explain the process by which it takes a snapshot and testify the screenshots were not faked, the material could be thrown out at a later date. But assuming that the Internet Archive continues to use the same system as it does now, it could arguably meet the standard for criminal evidence in certain circumstances.

Inside Internet Archive: 10PB+ of storage in a church... oh, and a little fight to preserve truth

READ MORE →

At some point, we imagine, it will no longer be necessary for there to be a witness, and the Internet Archive will stand up as a wholly legitimate source of past online activity.

As for the case itself, back in 2014, Gasperini managed to infect more than 150,000 computers – most of them in the US – with malware he created that exploited an unpatched hole in storage devices running QNAP's software.

It then installed malware that did five things: set up a super-user account; patched the hole; stole system username and passwords; send clicks to online ads; and scanned for other computers to create a botnet to be used for future denial-of-service attacks.

Prosecutors found a range of evidence against Gasperini. It tracked the servers hosting the malware back to him and found a test copy of the virus in his personal email. But a key part of the evidence was that websites hosting advertisements that his malware clicked on were registered under his name – as were the advertising deals he cut for those ads.

Archive

That's where the snapshots of what those websites looked like in the past came into play, especially after Gasperini was able to delete his Google email account and his Facebook account after his arrest and somebody – presumably under his instruction – also found and erased his hard drives at his home. The archives effectively acted as business records.

Gasperini was charged with computer intrusion with intent to defraud, wire fraud and money laundering. After a seven-day jury trial, he was acquitted of the felonies but was convicted of computer intrusion. At sentencing, the judge said the government had proven that Gasperini had committed the felony offenses and considered that when calculating his punishment: 63 to 78 months in jail. His sentence was capped at one year in jail, however, since he was only convicted of a misdemeanor.

Gasperini appealed that conviction, arguing three things: that the law under which he was convicted was too vague because the terms "access", "authorization" and "information" were not defined and the definition of "protected computer" is overbroad; that the Italian police were acting under the instruction of US police when they raided his house and so should have followed American standards for search; and that the Wayback Machine's snapshots should not be accepted as evidence.

The appeals court rejected all three arguments. ®

OpenSSL patches crash-me bug triggered by rogue certs

Bad data can throw vulnerable apps and services for an infinite loop

Brandon Vigliarolo Tue 15 Mar 2022 // 20:40 UTC

A bug in OpenSSL certificate parsing leaves systems open to denial-of-service attacks from anyone wielding an explicit curve.

The vulnerability stems from a bug in the BN_mod_sqrt() function, which the OpenSSL team said is used to parse certificates that "contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form." As it turns out, all you need to do to trigger an infinite loop in BN_mod_sqrt() is hand an OpenSSL-based application or service a certificate with invalid explicit curve parameters.

This parsing happens prior to verification of the certificate's signature. Slip a bad certificate to any app or server using BN_mod_sqrt() to parse certs, and the software will get caught in the loop and stop working.

CONTINUE READING

Microsoft Azure DevOps revives TLS 1.0/1.1 with rollback

Planned deprecation didn't go as planned, cloud biz aims to try again at the end of March

Thomas Claburn in San Francisco Tue 15 Mar 2022 // 19:24 UTC

Microsoft's Azure DevOps team has undone the deprecation of outdated Transport Layer Security (TLS) that occurred at the end of January