

CRYPTOME

24 July 2014

Full docket text:

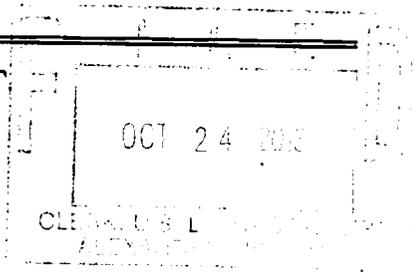
Case unsealed as to Lauri Love (krob,)

PACER Service Center			
Transaction Receipt			
07/24/2014 19:38:36			
PACER Login:		Client Code:	
Description:	History/Documents	Search Criteria:	1:13-mj-00657-TRJ
Billable Pages:	1	Cost:	0.10

UNDER SEAL

AO 91 (Rev. 08/09) Criminal Complaint

UNITED STATES DISTRICT COURT
for the
Eastern District of Virginia



United States of America)

v.)

LAURI LOVE)

a/k/a "nsh", a/k/a "route", a/k/a "peace", a/k/a "shift")

Case No. 1:13-mj-657

UNDER SEAL

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.
On or about the date(s) of October 2012 through August 2013 in the county of Loudoun and elsewhere in the
Eastern District of Virginia and elsewhere, the defendant(s) violated:

Code Section

Offense Description

18 U.S.C. § 371

Conspiracy

This criminal complaint is based on these facts:

SEE ATTACHED AFFIDAVIT OF FBI SPECIAL AGENT JAMES R. MACKIE

Continued on the attached sheet.

Reviewed by AUSA/SAUSA:

Jay V. Prabhu and Ryan K. Dickey

Complainant's signature

James R. Mackie, Special Agent

Printed name and title

Federal Bureau of Investigation

Sworn to before me and signed in my presence.

Date: 10/24/2013

/s/Thomas Rawles Jones, Jr.

Judge's signature

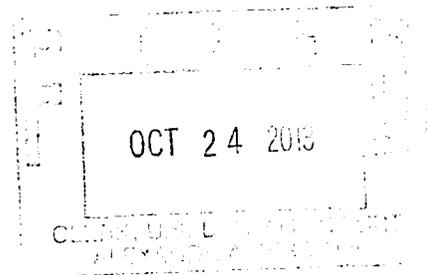
The Honorable T. Rawles Jones, Jr.,
United States Magistrate Judge

Printed name and title

City and state: Alexandria, Virginia

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



UNITED STATES OF AMERICA

v.

LAURI LOVE

also known as "nsh"
also known as "route"
also known as "peace"
also known as "shift"

Defendant

Criminal No. 1:13-mj-657

UNDER SEAL

**AFFIDAVIT IN SUPPORT OF
CRIMINAL COMPLAINT AND ARREST WARRANT**

I, James R. Mackie, being duly sworn, hereby depose and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since May of 2004. I am currently assigned to a cybercrime squad, where my duties include the investigation of crimes involving abuse and fraud relating to computers, including violations of 18 U.S.C. § 1030. As a Special Agent, I have received training in, and am authorized to investigate, crimes involving computers and computer intrusions.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show that there is sufficient probable cause for the requested arrest warrant and criminal complaint, and does not set forth all of my knowledge about this matter.

3. This affidavit is submitted in support of an arrest warrant and criminal complaint, charging the defendant, LAURI LOVE, also known as "nsh," "route," "peace," and "shift" (hereinafter "LOVE"), with conspiring with others known and unknown to the government to knowingly cause the transmission of a program, information, code, or command,

and, as a result of such conduct, intentionally cause damage without authorization, to a protected computer, in violation of 18 U.S.C. § 371 in furtherance of 18 U.S.C §§ 1030(a)(5)(A) and (c)(4)(B). The offense caused loss to persons during a 1-year period resulting from LOVE's course of conduct affecting protected computers aggregating at least \$5,000 in value, in violation of § 1030(c)(4)(A)(i)(I), and caused damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security, in violation of § 1030(c)(4)(A)(i)(V).

4. LOVE is a citizen of, and currently resides in, the United Kingdom.

5. Pursuant to 18 U.S.C. § 1030(e)(2), the term "protected computer" means either a computer exclusively for the use of the United States Government, or, in the case of a computer not exclusively for such use, used by the United States Government and the conduct constituting the offense affects that use by or for the Government, or a computer which is used in or affecting interstate or foreign commerce or communication. Pursuant to § 1030(e)(8), the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information. Pursuant to § 1030(e)(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service. Pursuant to § 1030(e)(12), the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

A. Manner and Means of Conspiracy

6. Between approximately October 2012 and August 2013, LOVE, together with individuals known and unknown to the United States, accessed without authorization protected computers belonging to the United States Department of Health and Human Services,

United States Sentencing Commission, Regional Computer Forensics Laboratory, and United States Department of Energy. LOVE and his conspirators gained unauthorized access to the protected computers by exploiting a known vulnerability in Adobe ColdFusion. Put simply, ColdFusion is computer software designed to build and administer websites and databases. The vulnerability, which has since been corrected, allowed LOVE and his conspirators to access protected areas of the victims' computer servers without proper login credentials — in other words, to bypass security on the protected computers. After gaining unauthorized access to the protected computer servers, LOVE and his conspirators uploaded password-protected files to the protected computer servers. These password-protected files were accessible through ordinary web browsers and served as custom file managers for ColdFusion applications running on the protected computer servers. The file manager provided LOVE and his conspirators with administrator-level access to the protected computer server, which included the capabilities of uploading and downloading files, as well as creating, editing, removing, and searching for data.

7. In or about October of 2012, LOVE and his conspirators gained unauthorized access to a protected computer. LOVE and his conspirators originated their attack from an Internet domain, which subscriber and financial records have confirmed was owned by LOVE. These records further show that LOVE paid for the domain with a PayPal, Inc. account registered with his e-mail address, lauri.love@gmail.com. Law enforcement has also obtained records showing that LOVE's PayPal payment for the domain originated from an Internet Protocol address associated with LOVE's residence in the United Kingdom.

8. Law enforcement has also obtained online conversations between LOVE and his conspirators, in which LOVE used the online nicknames "nsh," "route," "peace," and "shift" during the relevant time period. During these conversations, LOVE and his conspirators

discussed the unauthorized access of protected computers, sometimes in real time while committing the offense. These protected computers belonged to the United States Department of Health and Human Services, United States Sentencing Commission, Regional Computer Forensics Laboratory, and United States Department of Energy.

9. In furtherance of the conspiracy, a member of the conspiracy committed at least one overt act in the Eastern District of Virginia, including but not limited to the following:

B. Unauthorized Access of United States Department of Health and Human Services' Protected Computers

10. The Department of Health and Human Services ("HHS") is a cabinet-level department in the executive branch of the United States Government. Its principal purpose is to protect the health of all Americans and provide essential medical services. The Health Resources and Services Administration ("HRSA") is an agency of HHS and is responsible for providing access to health care for people who are uninsured, isolated, or medically vulnerable. The National Institutes of Health ("NIH") is an agency of HHS and is the largest source of funding for medical research in the world.

11. On or about December 24, 2012, LOVE and his conspirators gained unauthorized access to HHS protected computers. At the time, these protected computers were located in Sterling, Virginia, within the Eastern District of Virginia, and contained information for the HHS websites ask.hrsa.gov and report.nih.gov. LOVE's actions caused more than \$5,000 in loss to HHS.

12. On or about December 24, 2012, in an online conversation obtained by law enforcement, LOVE (through the nickname "shift") and his conspirators discussed the unauthorized access of HHS protected computers. LOVE said, "Trying to pwn [<http://www.ask.hrsa.gov>]" . After successfully gaining unauthorized access to the protected

computer, LOVE claimed, “oh so much to do..”, but “i will behave though and not autopwn many”, “because need to keep technique under wraps”. In my experience and in this context, the word “pwn” is a slang term for gaining access to, or control of, a system.

C. Unauthorized Access of United States Sentencing Commission’s Protected Computers

13. The United States Sentencing Commission (the “Commission”) is an independent agency in the judicial branch of the United States Government. Its principal purposes are to establish sentencing policies and practices for the federal courts, including guidelines to be consulted regarding the appropriate form and severity of punishment for offenders convicted of federal crimes; to advise and assist Congress and the executive branch in the development of effective and efficient crime policy; and to collect, analyze, research, and distribute a broad array of information on federal crime and sentencing issues, serving as an information resource for Congress, the executive branch, the courts, criminal justice practitioners, the academic community, and the public.

14. Beginning on or about December 25, 2012, and continuing through on or about January 27, 2013, LOVE and his conspirators gained unauthorized access to the Commission’s protected computers. After gaining unauthorized access, LOVE and his conspirators altered the website to display a video that criticized the guidelines with respect to Internet-related crimes. At the time, these protected computers were located in Sterling, Virginia, within the Eastern District of Virginia, and contained the Commission’s website, www.ussc.gov. The website provided to the public a wide selection of information, such as federal sentencing statistics by state and district, as well as materials, such as current and past versions of the sentencing guidelines. As a result of the intrusion and defacement, the USSC website was unavailable to the public for roughly three weeks. LOVE’s actions caused more than \$5,000 in loss to USSC, and the

protected computers damaged by LOVE were used by the United States Government in furtherance of the administration of justice.

15. On or about January 24, 2013, in an online conversation obtained by law enforcement, LOVE (through the nicknames "route" and "peace") and his conspirators discussed the unauthorized access of USSC protected computers. LOVE made the following statements: "found a whole bunch more shit on the ussc.gov hoster's network", "trying to leave a few ways in", "before we drop the bomb". LOVE also said, "will be needing help with ussc[.gov] today/tonight", "we aiming to go public for 5am EST == 11am tomorrow UK". In addition, LOVE said, "the script is finalised and the video will be ready tonight", apparently referring to the defacement video.

D. Unauthorized Access of Regional Computer Forensics Laboratory's Protected Computers

16. The Regional Computer Forensics Laboratory ("RCFL") is a national forensics laboratory and training center devoted to the examination of digital evidence in support of criminal investigations. The Federal Bureau of Investigation oversees the operations of the various RCFL offices.

17. Beginning on or about January 11, 2013, and continuing through on or about February 14, 2013, LOVE and his conspirators gained unauthorized access to the RCFL's protected computers. At the time, these protected computers were located in Sterling, Virginia, within the Eastern District of Virginia, and contained the RCFL's website, www.rcfl.gov. Through the unauthorized access, LOVE and his conspirators successfully stole the personal information, including names, phone numbers, and e-mail addresses, of RCFL and FBI employees. LOVE's actions caused more than \$5,000 in loss to RCFL, and the protected

computers damaged by LOVE were used by the United States Government in furtherance of the administration of justice.

18. On or about February 11, 2013, in an online conversation obtained by law enforcement, LOVE (through the nickname “peace”) and his conspirators discussed the unauthorized access of RCFL protected computers. LOVE made the following statements: “I think we should backdoor rcfl.gov”, “remote computer forensics [lab]”, “can probably get good infos from people who use it”.

E. Unauthorized Access of United States Department of Energy’s Protected Computers

19. The Department of Energy (“DOE”) is a cabinet-level department in the executive branch of the United States Government. Its mission is to ensure America’s security and prosperity by addressing its energy, environmental, and nuclear challenges through science and technology solutions.

20. Beginning on or about July 24, 2013, and continuing through on or about August 8, 2013, LOVE and his conspirators gained unauthorized access to DOE protected computers. At the time, these protected computers were located in Maryland and contained the personal information of DOE employees. Through the unauthorized access, LOVE and his conspirators successfully stole the personal information of numerous Virginia residents, including residents of the Eastern District of Virginia. LOVE’s actions caused more than \$5,000 in loss to DOE.

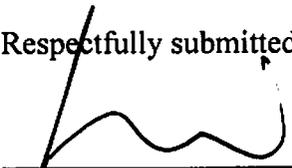
21. On or about July 26, 2013, in an online conversation obtained by law enforcement, LOVE (through the nickname “peace”) and his conspirators discussed the unauthorized access of DOE protected computers in real time during the offense. LOVE commented, “they [the DOE] must have about 30k employees[,]” and he then copied the personal information of various employees from the protected computer to the online

conversation. The personal information included the names, phone numbers, and e-mail addresses of the employees.

F. Conclusion

22. Based on the foregoing, there is probable cause to believe that between approximately October of 2012 through August of 2013, within the Eastern District of Virginia and elsewhere, LAURI LOVE conspired with persons known and unknown to the government to violate 18 U.S.C. 1030(a)(5)(A) and (c)(4)(B).

Respectfully submitted,



James R. Mackie
Special Agent, Federal Bureau of Investigation

Subscribed and sworn to before me on October 24, 2013

/s/Thomas Rawles Jones, Jr.

The Honorable T. Rawles Jones, Jr.
United States Magistrate Judge

Submitted by Jay V. Prabhu and Ryan K. Dickey
Assistant United States Attorneys