UNITED STATES DISTRICT COURT

DISTRICT OF NEW MEXICO

UNITED STATES OF AMERICA
V.

Devon Lynn Townsend
7504 Via Serenita SW
Albuquerque, NM 87121

(Name and Address of Defendant)

CRIMINAL COMPLAINT

Case Number: 06M 569

I, the undersigned complainant state that the following is true and correct to the best of my knowledge and belief. On or about 11/15/2006 (Date) in Bernalillo County, in the _____ District of New Mexico defendant(s) did,

(Track Statutory Language of Offense)

Intentionally intercepted and endeavored to intercept wire, oral, and electronic communications,

in violation of Title 18 United States Code, Section(s) 2511(1)(a).

I further state that I am a(n) DCIS Special Agent (Official Title) and that this complaint is based on the following facts:

See attached affidavit

Continued on the attached sheet and made a part of this complaint: ☑ Yes ☐ No

Signature of Complainant

Printed Name of Complainant

Sworn to before me and signed in my presence,

11/17/06 (Date) at Albuquerque (City) NM (State)

Alan C. Torgerson (Name of Judge) US Magistrate Judge (Title of Judge) Alan C. Torgerson (Signature of Judge)

COMPLAINT AFFIDAVIT

I, Jeffery E. Fauver, being duly sworn, hereby declare and state:

Background

1. I am a Special Agent (SA) for the Department of Defense (DoD), Office of Inspector General, Defense Criminal Investigative Service (DCIS), assigned to the Albuquerque Post of Duty. I have been employed by the DCIS for over 19 years, and I have been assigned to the Albuquerque, NM office since 1990. During my career as a SA with the DCIS, I have been assigned to investigate numerous crimes involving DoD interests, including computer crimes. I have participated in investigations involving the execution of search and seizure warrants, which have resulted in the seizure of computer-related equipment, media and data files evidencing fraud and other criminal activities. As a Computer Crimes SA, I have received specialized training in the investigation of computer, telecommunications, and other "high technology" crimes impacting the DoD.

2. As a DCIS Special Agent, I am conducting an investigation into allegations that Devon L. Townsend, an Albuquerque, NM, resident, currently employed at Sandia National Laboratory (SNL), Kirtland Air Force Base, NM, is using computers to engage in criminal activities. This affidavit is made in support of a criminal complaint for violations of Title 18 United States Code, Section 1028(a)(7), Fraud and related activity in connection with information; Section 1030(a)(2), Fraud and related activity in connection with computers; Sections 2319A, 2319(c)(1) and 2319(c)(2), Unauthorized

fixation of and trafficking in sound recordings and music videos of live musical performances; Section 2511(1)(a) and (d), Interception and disclosure of electronic communications prohibited; Section 2701, and Unlawful access to stored communications. The information contained in this affidavit was obtained through my investigative activity as well as from information provided by other investigators working jointly on this case.

Computer and Internet Term Descriptions

3. For the purposes of this affidavit, the following terms for computer and Internet related items are used and are described below:

Address Book - Usually part of an email program or web site, stores names and information in a manner similar to traditional address books;

AOL – America On Line, an Internet Content and Service Provider;

Briefcases – Generally are small, personalized storage areas on some providers systems;

Chat – An online area or program that works through an Internet connection allowing people to text communicate in real time;

Clubs – On line groups operating from a particular area on or through a service provider's site;

Cookie – A parcel of text sent by a server to a web browser and then sent back unchanged by the browser each time it accesses that server. Used for authenticating, tracking, and maintaining specific information about users;

Cyberspace – A term used to describe the Internet and other digitally connected sites;

Digital Image – Usually describes a photo or image that has been rendered to be electronically readable and displayed on a device, such as a computer, television, or cell phone;

EBay – An online marketplace used to buy and sell goods;

E-mail – Electronic mail, letters or messages that can be sent from one user to another and read on or off line;

Forensic Image – A bit by bit copy of a hard drive or other piece of digital media at a certain point in time;

Founder – Usually refers to someone who establishes a group or chat area within a web site;

Groups – Refers to people coming together through the Internet based on similar interests or other commonalities;

Hack – To gain unauthorized access into a computer system by means of manipulating computer code

Home Page – A default Internet site that is brought up in an Internet web browser;

IP Address – Internet Protocol Address, a unique address through which a computer connects to the Internet. Only one computer system at a time can connect to the Internet on a given IP address;

Internet Service Provider – Provides a connection from a user's computer to the Internet;

Instant Messenger – See chat;

.jpg – A commonly used image file format

Member – Someone who is part of or participates in a group in an online area;

PayPal – An Internet site that provides a means for persons to transfer monies for purchases made online;

Proxy Server – Serves as a private or public gateway allowing other computers to pass through it to connect to the Internet;

Screen Name – A name that is usually defined by the user to login to a system or web site, often associated with email addresses or email programs;

Probable Cause

4. On or about October 12, 2006, your affiant received information from SA Kevin Levy, United States Secret Service (USSS), Mobile Resident Office, Mobile, AL, regarding an identity theft complaint that he had received through K. Gus Dimitrelos, Director of Digital Evidence, Alabama Computer Forensics Laboratory, Spanish Fort, AL. According to SA Levy, an individual named Talinda Bennington reported to them that she was concerned because an unknown person, without authorization, had somehow accessed their Verizon Wireless ("Verizon") telephone account used by her and her husband, Chester Bennington. Chester Bennington is a nationally known public figure because he is the lead singer of the highly popular band Linkin Park. [Agents believe that the unauthorized access to the Bennington's Verizon account was apparently made using a computer to "hack" into Verizon's computerized account and billing records.] Both Talinda Bennington and Chester were very concerned about the Verizon incident due to other indications that the individual responsible for the unauthorized access to their Verizon account had also obtained other personal information about them. The Bennington's explained that someone had gained access to their PayPal and Verizon

accounts because they had received notices from both entities that their passwords were constantly being changed. As an example, their password was changed on one occasion to "Who is doing this to you?" Talinda Bennington characterized recent unusual events as being attributable to a stalker because the type of personal information possessed by this unknown person was not publicly available. Other examples include postings on a band related website, Linkin Lady, where a website user posted confidential information concerning the Bennington's children and wedding, which caused the user to be removed from the website. On another occasion, an individual impersonated Talinda Bennington by calling Talinda's personal security guard and asking him for Chester Bennington's ex-wife's e-mail address.

5. SA Levy also related to your affiant that records he had in his possession indicated the unauthorized electronic access to the Bennington's Verizon account could be traced to the source Internet Protocol (IP) address of 134.253.26.4, with a connection time at approximately 8:19 a.m. Pacific Standard Time, on September 25, 2006. SA Levy requested SA Fauver's assistance to verify the location of the computer network associated with that IP address. An Internet query of the computer network domain associated with the IP address 134.253.26.4 disclosed that the computer corresponding to that IP address was within a network operated at Sandia National Laboratories (SNL) located on Kirtland Air Force Base (KAFB), NM. SNL is a federally funded national laboratory that is overseen by the United States Department of Energy.

6. SA Levy later provided more information about a second IP address of

68.35.185.110 which had apparently been used to access the victim's Verizon account. An Internet query of the computer network domain associated with the IP address 68.35.185.110, disclosed that the computer corresponding to that IP address was within a network domain operated by Comcast Cable Communications (Comcast), Incorporated.

7. On October 13, 2006, your affiant communicated with SA Goward of the Department of Energy (DoE), Office of Inspector General (OIG), Technology Crimes Section (TCS). Your affiant informed SA Goward that during a DCIS investigation, a SNL IP address was identified as being used to gain unauthorized access to an account belonging to Chester and Talinda Bennington, Verizon wireless customers. The IP address, date and time was identified by DCIS as being 134.253.26.4 on 9/25/06 at approximately 8:19 am PDT, meaning that a computer at SNL was used to gain unauthorized access to the account. The intruder was alleged to have used the SNL IP address to connect to the Verizon wireless server and break into the account and change several key pieces of information belonging to the Benningtons.

8. On October 13, 2006, SA Goward contacted Mr. Roger Suppona, computer security manager, at SNL. SA Goward explained the allegations and related the IP address that was alleged to have been used. Mr. Suppona stated that this IP address belonged to one of nine proxy servers that were used at SNL. Mr. Suppona stated that he would need more information relating to the attack in order to properly identify the computer used.

9. On October 13, 2006, your affiant provided SA Goward with the information relating to the Verizon wireless IP address and domain names that were alleged to have been accessed by the SNL computer.

10. On October 18, 2006, SA Goward contacted Mr. Suppona with the information provided by your affiant. Mr. Suppona researched the issue and identified the network responsible for the activity. Mr. Suppona stated that this was a terminal server network designated TS01MFGCX, which was an unclassified computer belonging to the Technology and Manufacturing group. However, the computer at issue is only accessible by a limited number of personnel because of its location in a secure area of SNL requiring a coded passcard to gain entrance. Mr. Suppona also explained that all users on the SNL computer network are assigned a unique username. To gain access to the SNL computer network, each individual must enter their username and password that is supposed to be known only to that user.

11. SA Goward requested that a forensic image of the terminal server be made and that the Internet logs and active users be provided as well. Mr. Suppona stated that he would arrange for Mr. Kevin Nauer, Computer Security, SNL, to make an image of the terminal server.

12. On October 24, 2006, SA Goward received via FedEx shipment number 858 225 664 380 containing the computer log and forensic image of the SNL terminal server # TS01MFGCX. The forensic image was contained on two DVD's and the log on one

CD. Also in the package was a listing of active users for September 25, 2006 and an image summary sheet provided by Mr. Kevin Nauer, the forensic examiner making the image.

13. SA Goward reviewed the listing of active users by username on September 25, 2006, for terminal server #TS01MFGCX for September 25, 2006, and found seven users had logged onto that particular terminal server that day. SA Goward also examined the log files relating to terminal server #TS01MFGCX and found that on the date and time previously provided by your affiant , a user of the terminal server did connect to the Verizon Wireless Internet website.

14. On October 26, 2006, SA Goward began the process of loading the forensic image of the SNL terminal server #TS01MFGCX onto a government owned forensic computer. The forensic image of the terminal server was loaded into the Access Data Forensic Tool Kit version 1.60.

15. The SNL terminal server is an unclassified computer system that is owned by the United States Department of Energy and operated by SNL. The terminal server services multiple users within the Technology and Manufacturing group at SNL. Computers in operation at SNL display a warning banner when users logon. The warning banner below was found on the terminal server computer:

> SF 2902-NTU (10-2004) WARNING NOTICE TO USERS This is a Federal computer system and is the property of the United States Government. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy. Any or all uses of this system and all files on this system may

be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized Sandia National Laboratories, Department of Energy, and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of Sandia National Laboratories or the Department of Energy personnel. Use of Sandia National Laboratories computing equipment and information shall be in compliance with SNL business rules (CPSR400.2 series). These business rules are available on the internal web at the following URL: http://www-irn.sandia.gov/policy/brnumbrs.htm#information Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. Press the "OK" button to indicate your awareness of and agreement with the terms and conditions of this warning notice. If you do not agree with these terms and conditions DISCONTINUE all efforts to access or utilize SNL computing equipment and information.

16. On or about October 29, 2006, your affiant contacted the Albuquerque offices of Comcast, and asked them to verify the user assigned to IP address 68.35.185.11 during the August 2006 time period. The IP address 68.35.185.110 was confirmed as a Comcast IP address. Subsequent to the initial contact with Comcast, additional information was obtained from the Comcast Legal Response Center confirming the IP address 68.35.185.110 was being used by the subscriber Devon Townsend, from July 30, 2005 through August 16, 2006, at the address 7504 Via Serenita SW, Albuquerque, NM, 87121-2131. For the time period August 19, 2006, the IP address being used by Townsend was 69.252.213.118.

17. Your affiant has confirmed that an individual named Devon Townsend is employed at SNL in Albuquerque as a tradesperson. Townsend works in the Technology and Manufacturing group and has access to the terminal server network computer designated as TS01MFGCX.

18. On October 30, 2006, SA Goward began examining the user accounts for users logged onto SNL Terminal Server #TS01MFGCX on September 25, 2006. While examining the accounts, SA Goward observed that the "dltowns" account appeared to stand apart from the other users logged on that day. From information provided by SNL, SA Goward was able to determine that the "dltowns" (Townsend) account belonged to a SNL employee, Devon L. Townsend. SA Goward noticed that the Townsend account had a large amount of Internet activity for a single day and appeared to have significantly more Internet activity than any of the other accounts. SA Goward observed that the Temporary Internet Files settings appear to be set to keep a single day at a time. SA Goward also noticed several references to websites relating to the rock band Linkin Park, Chester and Talinda Bennington, and underground music trading in the account.

19. SA Goward conducted an Autotrack search for a Devon L. Townsend in the Albuquerque, New Mexico area. AutoTrack is an Internet based database tool that is available to authorized law enforcement officials, which have an account with the company, to electronically access information pertaining to individuals and companies in the United States, to include public information, current addresses and other related personal identification data. The Autotrack search resulted in one Devon L. Townsend being listed in the Albuquerque, New Mexico area. The Autotrack search provided the below listed information for Devon L. Townsend:

Name: Devon L. Townsend
SSN: 525-47-0578
Address: 7504 VIA SERENITA SW, ALBUQUERQUE, NM 87121
DOB: 02/28/1979

DL #: 005700370 EXP. 03/28/2007

20. On October 31, 2006, your affiant contacted SA Goward and explained that when the Bennington's Verizon account had been compromised, the intruder had also changed the email address in the account from ctbennington@mac.com to a false email address of talindab@aol.com. In addition, records obtained by SA Levy indicate that the intruder had connected to the Verizon server on September 25, 2006 at 8:18 am Pacific Standard Time, and using the ctbennington login name and profile, was able to change the password denying the Bennington's access to their account. The intruder then used the ctbennington login name and new password to gain access to the account.

21. After receiving this information SA Goward searched for variations of the email addresses, and account names provided. This search revealed several instances for talindab@aol.com as well as talindab@yahoo.com in the Townsend account. An instance of the ctbennington@mac.com address was also found inside an Internet cookie from PayPal.com in the Townsend account at SNL. SA Goward observed in a search of the forensic image that the search term "talindab@aol.com" appeared numerous times on the Townsend account in the form of cookies from AOL. The email address talindab@yahoo.com appeared numerous times as partially recovered emails. Based on the initial examination, SA Goward believes that Townsend was accessing the talindab@yahoo.com email account using a government computer. Based on his experience in investigating computer crimes, SA Goward believes that Townsend uses the talindab@aol.com email address to redirect and capture the emails and other information belonging to the Benningtons. SA Goward also learned from SA Levy that

the talindab@yahoo.com email address is an email address belonging to Talinda Bennington.

22. On November 1, 2006, SA Goward was searching through the "Desktop" folder in the Townsend account when he observed the file "ct_august2006.pdf". After opening the file, SA Goward observed that this file contained a 34 page Verizon Wireless bill belonging to the Benningtons. Inside the 34 page document were detailed billing records for five phone numbers belonging to Chester and Talinda Bennington for the month of June 2006 until July 2006. The bill showed approximately 718 records for incoming or outgoing calls on the Benningtons account. Another copy of the file was also found under the "Desktop" folder under the filename of July 2006.pdf.

23. While looking through the files in the "Desktop" folder numerous photographs were found that appear to be related to the Bennington's and their friends. The files show photographs of the Bennington's and their friends, apparently in Japan and other locations as well as photographs of the Benningtons children. Based on experience, SA Goward believes that the majority of the photos found were taken by a digital camera perhaps on a cellular phone, and are not photos that would appear to be publicly available or that should be in the possession of Townsend.

24. After reviewing the photographs identified on Townsend's desktop, on November 14, 2006, Talinda Bennington identified seventy-eight (78) photographs which she had taken with a personally owned digital camera and transmitted via email and the

internet to a single and specific receiving party. Therefore the contents of this data recovery on Townsend's desktop provides additional examples of intercepted communications which appear to have been illegally intercepted, downloaded and stored without authorization. Some clear examples, but not all of the images Talinda Bennington described on November 14, 2006 with regard to digital camera image are listed as the .jpg photographs named below:

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Desktop\pix\Picture001.jpg;

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Desktop\pix\Photo000.jpg

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Desktop\pix\P8150245.jpg

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Desktop\pix\P81502381.jpg

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Desktop\pix\P8150238.jpg

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Desktop\pix\P81502371.jpg

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Desktop\pix\P8150237.jpg

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Desktop\pix\P81502361.jpg

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Desktop\pix\P8150236.jpg

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Desktop\pix\P8150232.jpg

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Desktop\pix\P8150231.jpg

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Desktop\pix\P8150229.jpg

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Desktop\pix\P8150227.jpg

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Desktop\pix\P8150223.jpg

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Desktop\pix\P8150222.jpg

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Desktop\pix\P1010209.jpg

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Desktop\pix\P1010206.jpg

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Desktop\pix\P1010205.jpg

25. Talinda Bennington has also identified five (5) other .jpg photographs, discovered on the Townsend account at SNL, which Talinda Bennington took with a personally owned cellular telephone camera and transmitted via email, cellular network, and/or and the internet to a single and specific receiving party. Therefore the contents of this data recovery on the subject's desktop further serve as additional examples of intercepted electronic communications which have been captured, downloaded and stored without authorization. Some clear examples, but not all of the images Talinda Bennington described on November 14, 2006, regarding these camera phone images are identified below:

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Desktop\pix\Photo_070.jpg

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Desktop\pix\Photo_07.jpg

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Desktop\pix\P8150252.jpg

I07TC002\ (TS01MFGCX, 134.253.78.205)-0\D\Documents and Settings\dltowns\Personal\My Pictures\Club Tattoo\Club Tattoo 4.22.06\Sean & Chester.jpg

I07TC002\ (TS01MFGCX, 134.253.78.205)·0\D\Documents and Settings\dltowns\Personal\My Pictures\Kids\ty in car seat.j

26. On November 2, 2006, SA Goward found two additional Verizon Wireless bills relating to the Benningtons for the months of March and September 2006 on the Townsend account. Additional searching by SA Goward also revealed three Verizon Wireless bills for Townsend. On examining the Townsend phone records for the month of April to May, 2006, SA Goward observed nine calls from Townsend's Verizon Wireless phone to Chester Bennington's cell phone.

27. Talinda Bennington also reported that she had received anonymous phone calls during August of 2006 where the person called her a "whore" and during another call made the statement "I know where you live." On the morning of September 26, 2006, Talinda Bennington received a phone call from a female sounding caller that made statements such as "I know where you live", "I watch you and your kids", and "I have complete control of your life."

28. SA Goward identified text and music lists found in the Townsend account as matching those found on a website Townsend appears to control which is located at the address of "db.etree.org". Using this website Townsend appears to be actively trading and bartering bootleg music and videos. This list of bootleg music and videos includes entries for Chester Bennington's band, Linkin Park, as well as other popular groups organized by date, state, city, venue, and media type. In the comments section of the left margin, Townsend discusses her preferences for trades and issues related to media types

and also states that the shows are captured by concertgoers and not professionals. SA Goward noted that Townsend also appeared to be communicating with other bootleg music traders using her government computer.

29. Effective as of the most recent website update on October 30, 2006, to the site "db.etree.org", information has been retrieved from digital sources indicating the subject has uploaded for purposes of distribution, multiple labels and/or digital reproductions of copyrighted works in excess of $2,500 retail value. On November 14, 2006, entertainment attorney Daniel B. Hayes stated that each CDR and/or DVD have an average retail market value of $20.00 or greater. These titles are posted on the website "db.etree.org", under the heading "music list for Devon", and in part includes labels from the following musical bands and organizations:

Band/Label	Qty. of Label Titles	Retail Value
Linkin Park	111	$2,220
Linkin Park and Jay-Z	1	$ 20
The Cure	26	$ 520
Puddle of Mud	6	$ 120
Fort Minor	2	$ 40
	146	$2,920

30. On November 7, 2006, I received information from an Albuquerque Postal Inspector regarding mail recipients at the address 7504 Via Serenita SW, Albuquerque, NM, 87121-2131. Confirmation was provided that Townsend is receiving mail at that address.

31. On November 16, 2006, a federal search warrant was executed at Townsend's residence, 7504 Via Serenita SW, Albuquerque, NM, 87121-2131. During the search of Townsend's residence, various types of evidence were seized including posters of Linkin Park members, signed Linkin Park memorabilia, pictures of Townsend taken with Chester Bennington, bootlegged music and video CD/DVD's, concert schedules, copies of messages from Talinda and Chester Bennington's e-mail accounts, intercepted photographs from Talinda and Chester Bennington's e-mail accounts, and other items.

32. Townsend was interviewed at the DoE/OIG offices located near the facility where Townsend was working. After being advised of her right and signing a USSS Warning and Consent to Speak Form 1737B, Townsend confessed to her online hacking activity which led to the interception of the Bennington's email and other personal information. Townsend also admitted to her telephoning the Bennington's. When Townsend was asked on a scale of one through ten how threatened she thought the Bennington's would feel by her phone calls, she "rated it a ten" but she thought her actions only rated a 2. Townsend also prepared a signed statement outlining the methods she used to obtain unauthorized access to the Bennington's email accounts and other activity she engaged in during her attempts to remain in contact with the Bennington's while capturing their personal information.

33. Based upon the information set forth above, my training and experience, and that of other law enforcement officials with whom I have consulted with in this investigation to date, there is probable cause to believe that Devon L. Townsend has

committed violations of Title 18 United States Code, Section 1028(a)(7), Fraud and related activity in connection with information; Section 1030(a)(2), Fraud and related activity in connection with computers; Section 2319A, Unauthorized fixation of and trafficking in sound recordings and music videos of live musical performances; Section 2511(1)(a) and (d), Interception and disclosure of electronic communications prohibited; and Section 2701, Unlawful access to stored communications.

34. Because this affidavit is being submitted for the limited purpose of providing probable cause regarding a criminal complaint, I have not included every detail regarding my investigation or the joint DCIS/USSS/DOE-OIG investigation involving Devon Townsend.

Jeffery E. Fauver
Special Agent
Defense Criminal Investigative Service

Subscribed and sworn to before me this 17 day of November, 2006, in Albuquerque, NM.

United States Magistrate Judge