

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

SUPERIOR COURT OF THE STATE OF CALIFORNIA
COUNTY OF SACRAMENTO

**PEOPLE OF THE STATE OF
CALIFORNIA ,**

Plaintiff,

v.

GEORGE SAMUEL BRONK,

Defendant.

XRef#:

**DECLARATION IN SUPPORT OF
ISSUANCE OF ARREST WARRANT**

I, Peter L. Lockhart Jr., declare:

I am an investigator and peace officer employed by the Department of California Highway Patrol (CHP). I have been employed by the CHP since November of 1995. I am currently assigned to the CHP's Computer Crime Investigation Unit (CCIU) which is based out of CHP Headquarters in Sacramento and handles computer crimes involving state agencies, assets, employees and infrastructure statewide.

In November of 1995, I attended and graduated from the 27 week CHP Academy (Cadet Training Class IV-95). Training included instruction on patrol procedures, the investigation of criminal violations, traffic law, alcohol and drug law violations and traffic collision investigation.

1 Upon graduation from the academy, I was assigned to the CHP Redwood City Area office in San
2 Mateo County where I performed patrol duties. While investigating incidents on patrol, I
3 interviewed hundreds of victims, witnesses and suspects involved in criminal activity.

4 In 1998, I was assigned to the CHP Santa Cruz Area office in Santa Cruz County where I
5 continued performing patrol duties. While investigating incidents on patrol, I interviewed
6 hundreds of victims, witnesses and suspects involved in criminal activity. I assisted Santa Cruz
7 County Sheriff's Department, Watsonville Police Department and Santa Cruz Police Department
8 in the investigation of non-traffic crimes including assaults, thefts and gang activities.

9 In October 2003, I was assigned to the CCIU which investigates technology related crimes
10 related to State of California agencies, infrastructure and assets. In this position, I have
11 investigated incidents associated with peer-to-peer networks, child pornography, illegal network
12 access/intrusion ("hacking") and extortion by e-mail. While assigned to the CCIU, I have
13 received over 900 hours of specialized training in the preservation and examination of digital and
14 computer related evidence, including vender specific training on the forensic applications
15 available from Guidance Software and Access Data, as well as general computer crime
16 investigation/forensic training from the California Department of Justice, the National White
17 Collar Crime Center (NW3C) and the SANS (SysAdmin, Audit, Network, Security) Institute. I
18 have received interview and interrogation training from the Reid Institute and additional criminal
19 investigation training at the California POST (Peace Officer's Standards and Training), Robert
20 Presley ICI (Institute of Criminal Investigation) core course for criminal investigators. In July
21 2009, I completed training requirements mandated by California POST and was certified as a
22 Certified Computer Crime Investigator for the State of California. I am a member of
23 infrastructure protection groups including the FBI's InfraGard, the High Technology Criminal
24 Investigator's Association (HTCIA), and a joint CHP/FBI computer crimes task force.

25 The following information is either personally known to me or from the statements or
26 written reports provided by the identified law enforcement agencies or their officers or
27 employees.
28

Summary

From December 2009 through September 2010, George Samuel Bronk, accessed without authorization e-mail and Facebook accounts and published private information on the victims Facebook account.

E-mail accounts were accessed by using a feature which allows a user to recover a forgotten password. These accounts allow a series of security questions to be asked to the user attempting access. These security questions are often based on the account holder's personal life: mother's birth place, high school attended, favorite movie, favorite color, to list a few.

Bronk targeted Facebook accounts that listed personal e-mail addresses. He then attempted to access these e-mail accounts by "guessing" the security questions. Bronk used the victim's information posted on Facebook to assist in his "guessing." Bronk's "pass.txt" file indicates that he has compiled potential access information to over 3200 e-mail accounts.

Once Bronk gained access to the e-mail account he would search the account for nude or compromising photos. Bronk would then access the "forgot your password" link on the victim's Facebook account and request the password to be sent to the e-mail account he controlled. Bronk would then gain access to the victim's Facebook account and publish the nude or compromising photos that he harvested from the victim's e-mail account. In some cases Bronk would also e-mail these photos to the victim's entire e-mail address book.

Bronk's "nextfornav" folder indicates that he successfully accessed 172 email accounts and copied out nude or compromising photos. To date, 15 of these victims have been contacted and in the majority of these cases, Bronk published the victim's nude or compromising photos to the victim's Facebook profile. In one case Bronk extorted additional nude photographs from a victim by threatening to release photographs in his possession.

In addition to the unauthorized access of online accounts and theft of personal data, photographs, and videos, Bronk downloaded a large amount of child pornography photographs and videos, then saved the files to his desktop computer.

Initial Investigation

On August 3, 2010, I received and reviewed a package from Connecticut State Police (CSP) Trooper David Aresco containing a copy of an investigative report he compiled regarding a complaint from a resident of the state of Connecticut. The complainant alleged unauthorized access of several online accounts. The complainant was identified as Aili Alechnowicz.

On August 6, 2010, I contacted Trooper Aresco via telephone and spoke with him regarding the investigation. Based upon my review of the investigation package and my conversation with Trooper Aresco, I learned the following:

In April 20, 2010, Ms. Alechnowicz contacted the CSP reporting that an unknown person had taken control of her email account at @gmail.com and social networking page at www.facebook.com. The unknown person had somehow acquired nude photographs of Ms. Alechnowicz and posted the photographs on her Facebook page¹. Additionally, the unknown person sent an email on April 18, 2010, with the photographs to Ms. Alechnowicz's father and uncle. Ms. Alechnowicz eventually regained control of her Gmail and Facebook accounts, with no further incident.

On May 14, 2010, Trooper Aresco received the Gmail account subscriber and connection information from Google as a result of an Ex-parte he filed on April 25, 2010. The response included any *Internet Protocol (IP)² addresses used to access Ms. Alechnowicz's Gmail account before and after April 20, 2010, which was the day she was locked out. During review of the connection information, Trooper Aresco noted three separate IP addresses were listed. The first, was determined to be Ms. Alechnowicz's IP address. The second, 98.238.175.73, was listed by Gmail as successfully connecting to Ms. Alechnowicz's email account on April 18, 2010. A quick inquiry by Trooper Aresco determined the IP was registered to Comcast Cable and was in

¹ Facebook, a social networking site, allows the owner of the account to share information with friends or the public at large. The intruder, by accessing, controls the account and assumes the victims identity.

² An Internet Protocol address is a numerical label assigned to devices participating in a computer network. An IP address serves two principal functions: host or network interface identification and location addressing.

1 use in the Sacramento region. The third IP, 95.41.120.24, was unsuccessful in its attempt to log-
2 in to Ms. Alechnowicz's Gmail account. This IP was determined to be located in Poland and only
3 attempted to connect on April 22, 2010, after Ms. Alechnowicz had regained control of her
4 account.

5 On June 15, 2010, Trooper Aresco received an Ex-parte order response from Facebook,
6 containing connection information for Ms. Alechnowicz's Facebook account. Two IP addresses
7 were listed as successfully connecting to the Facebook profile during between April 17, 2010 and
8 April 22, 2010. Ms. Alechnowicz's assigned IP was listed as connecting from on each day from
9 the April 17 to April 22. The IP address assigned to Comcast Cable, 98.238.175.73 was captured
10 as logging in to Ms. Alechnowicz's account first on April 19 and then on April 20, the day the
11 nude photographs were uploaded.

12 On June 16, 2010, Trooper Aresco received an Ex-parte order response from Comcast
13 Cable he filed on May 23, 2010 for the IP address 98.238.175.73. The Comcast response listed
14 subscriber information for the user assigned to IP address 98.238.175.73: George Bronk, 5811
15 Our Way, Citrus Heights, CA 95610, assigned as of August 9, 2008.

16 Ms. Alechnowicz told Trooper Aresco that she did not know anyone named George Bronk
17 and that she had not given anyone with that name access to her online accounts. Furthermore, she
18 stated she did not know anyone at the address of 5811 Our Way, Citrus Heights, CA, and had not
19 given anyone at this address, copies of any photographs of her, nor had she approved anyone at
20 this address to upload photographs of her to her online accounts.

21 On September 24, 2010, I served a search warrant at 5811 Our Way, Citrus Heights, CA
22 95610. While serving the search warrant at the residence, I spoke with George Samuel Bronk,
23 George Patrick Bronk, Joyce Bronk and Grace Bronk. They all denied having anything do to with
24 the illegal activity associated with Ms. Alechnowicz.

25 **George Samuel Bronk's Admissions**

26 In a subsequent, non-custodial interview with George Samuel Bronk, he admitted to
27 accessing Ms. Alechnowicz' online account at Google.com and searching it for photographs. He
28 stated he gained access to Ms. Alechnowicz' online account at Facebook.com, and uploaded

1 photographs he located in her email account, to a gallery within her Facebook profile. Mr. Bronk
2 informed me that Ms. Alechnowicz' account was not the only time he had accessed other
3 people's email and social network sites, advising he had gained unauthorized access to other
4 Facebook accounts approximately six to twelve times and gained unauthorized access to other
5 email accounts approximately thirty times.

6 He advised he would search Facebook for profiles which included contact information
7 listing a web mail email address. He would go to the particular web mail provider and attempt to
8 login, using the email address he harvested off of Facebook. Depending on how the web mail
9 provider is set up, eventually he could access the forgotten password function, which is normally
10 a security question set-up by the user during account activation. He would then attempt to answer
11 the question. If he failed, he would move on to another email address or another person. If he
12 was successful, he would then return to Facebook and utilize the forgotten password feature for
13 the profile he was attempting to access by having Facebook send him a password to the already
14 accessed web mail account. He stated when he located photographs in the web mail accounts he
15 accessed, he would save the photographs to a folder on the desktop of his computer. He would
16 then send those photographs out to the email addresses in their contact list and if he had gained
17 access to their Facebook account, he would upload them to a gallery within the account.

18 During the search warrant service, Joyce Bronk advised me she and everyone else at the
19 house refer to her son, George Samuel Bronk, as "Geeg."

20 **Forensic Examination of Computers**

21 As part of this investigation I began a forensic examination of item #2 identified as a
22 CoolerMaster desktop computer with Western Digital Caviar Blue HDD. This computer was
23 located on the desk in George Samuel Bronk's bedroom, at 5811 Our Way, Citrus Heights, CA
24 95610.

25 I previewed the hard disk drive (HDD) installed in this computer and found photographs of
26 Ms. Alechnowicz saved within the folder located at: C:\Documents and
27 Settings\Geeg\Desktop\nextfornav\aaalechnowicz.

28 **"nextfornav" Folder**

1 While conducting a forensic analysis of the HDD installed in this computer, I navigated to
2 the folder at: C:\Documents and Settings\Geeg\Desktop\nextfornav. During the examination of
3 this location, I began documenting the multiple folders within the "nextfornav" folder and
4 observed there were 172 folders, each appearing to be named consistent with online screen/social
5 network/email address type names, and each containing photographs of nude and/or semi-nude
6 females.³ The "nextfornav" contained the storage folders for what appeared to be multiple
7 accessed accounts, as well as many uncategorized photographs.

8 **"pass.txt." File**

9 While I was documenting the "nextfornav" folder stored on the desktop area for the user
10 Geeg, I noticed a text file, also stored on the desktop, named "pass.txt." I viewed the "pass.txt"
11 file and observed it contained entries with email addresses, a date and what appeared to be some
12 type of data associated with the email address.

13 I searched the "pass.txt" file for Ms. Alechnowicz' information and located her email
14 address. I observed the date under Ms. Alechnowicz' email address which corresponded to her
15 date of birth (DOB).

16 I then searched the "pass.txt" file for the corresponding information for all folders located
17 within the "nextfornav" folder. I noticed the "pass.txt" file contained not only the email
18 address/date information entries for almost all of the "nextfornav" folders, but a large amount of
19 email address/date entries for many other unknown possible victims. I exported the "pass.txt" file
20 out and searched it for email addresses in general and found there were approximately 3200 email
21 address entries stored within the file. I extracted the email/DOB/personal data for each
22 corresponding folder from the "nextfornav" folder and further categorized the email addresses by
23 web mail provider.

24 I observed the information from the pass.txt file seemed to build from bottom to top. The
25 account information for the three accounts accessed during the online chat session listed
26 y*****@gmail.com first, "xogreen*****" next and "*****suicide" last. While

27 ³ As of the date of this warrant 15 out of the 172 folders have been associated with an
28 identified victim.

1 searching through the pass.txt file for the account information, I noticed what appeared to be
2 notes to the author of the file. In various locations, from the bottom of the file, to the top, I
3 located the following text notations:

4 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!400 MARK!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
5 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!500 mark!!
6 !!!!!!!!!!!!!!!!!!!!!700 mark!!
7 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!1000
8 MARK!!
9 !!!!!!!!!!!!!1200 mark!!!!!!!!!!
10 !!! 1323 MARK!!!!!!!!!!!!!!!!!!!!

11 I believe these notations indicate the progress Mr. Bronk was making at illegally attempting
12 to access email accounts and the associated Facebook accounts.⁴

13 **Other Identified Victims**

14 Lillian Moore

15 I spoke with Lawrence Kansas Police Department Detective Dean Brown, who advised on
16 June 14, 2010, his department received a complaint from Ms. Lillian Moore regarding her email
17 account at google.com (gmail) and online social network account at Facebook.com.

18 Detective Brown stated an unauthorized, unknown user gained access to Ms. Moore's email
19 account, located nude images and an erotic video file and uploaded the images to Ms. Moore's
20 Facebook page and sent the photographs to her email contacts. Additionally, the unknown user
21 sent a copy of the erotic video file to an amateur pornography web site, using her email account.

22 Detective Brown sent a subpoena to Facebook.com for IP connection information to Ms.
23 Moore's account. Facebook IP logs confirmed IP address of 98.238.175.73, which is the IP
24 address assigned to 5811 Our Way, Citrus Heights, CA, accessed Ms. Moore's account on June
25 14, 2010, at 0212 hours.

26
27 ⁴ As of the date of this warrant 28 out of the 3200 e-mail accounts have been associated
28 with an identified victim

1 I searched the "nextfornav" folder for evidence of the second reported victim, Lillian
2 Moore. I located a folder named which was named after the partial of the email address Ms.
3 Moore reported was accessed by an unauthorized user. Within the folder were nude and semi-
4 nude photographs of an adult female and two videos containing the female.

5 I searched the "pass.txt" file for Ms. Moore's information and located her email address and
6 her DOB.

7 Victoria Terry, a staff member of the Special Crimes Unit of the Attorney General's Office,
8 provided Ms. Moore with a copy of images recovered from the folder located within the
9 "nextfornav" folder that was associated with Ms. Moore. Ms. Moore confirmed that these were
10 her photos.

11 Detective Brown informed me that during his investigation, he determined at or around the
12 same time Ms. Moore's account were being accessed, several of her online friends' and their
13 friend's accounts were accessed in the same manner. During interviews with Bonnie Reynolds,
14 Sierra Tuttle, and Danielle Hart, Detective Brown learned all their online accounts were accessed
15 to various degrees on either June 13 or June 14, 2010.

16 Bonnie Reynolds and Danielle Hart

17 I further searched the "pass.txt" file for the email information of additional victims, Bonnie
18 Reynolds, Danielle Hart and Sierra Tuttle. I was able to locate email address/date information for
19 Ms. Reynolds and Ms. Hart in the file, although I noticed neither had a corresponding storage
20 folder for photographs in the "nextfornav" folder.

21 Danielle Hart reported an unknown unauthorized user locked her out of her email accounts,
22 @gmail.com and @yahoo.com, on June 14, 2010. Ms. Hart regained control of her Gmail
23 account later in the day on June 14, 2010 and her Yahoo account on June 17, 2010.

24 Bonnie Reynolds reported an unknown unauthorized user locked her out of her email
25 accounts, @hotmail.com and @gmail.com, on June 13 or June 14, 2010. Ms Reynolds advised
26 she realized she was also locked out of her Facebook account when she received a call from a
27 friend advising someone was using Ms. Reynold's account to post "hacking" messages onto Ms.
28 Moore's Facebook account.

1 Detective Brown filed a subpoena with Facebook for IP address connection information and
2 Facebook logs confirmed the account for Bonnie Reynolds was accessed by IP address
3 98.238.175.73⁵, on June 13, 2010, at 2350 hours.

4 Katie Amaral

5 Working with the "nextfornav" folder and the "pass.txt" file, I was able to assign an e-mail
6 address to the "nextfornav" folders since the folders were named consistent with online
7 screen/social network/email address type names. These e-mail addresses were then provided to
8 the Attorney General's Office.

9 Victoria Terry, a staff member of the Special Crimes Unit of the Attorney General's Office,
10 sent a questionnaire to these addresses. Victoria Terry related that she received a response from
11 Katie Amaral.

12 Katie Amaral reported an unknown unauthorized user locked her out of her email accounts,
13 @yahoo.com and @gmail.com, on June 23, 2010. Ms. Amaral advised she was also locked out
14 of her Facebook account and the intruder posted nude photos on her Facebook account that were
15 taken from her Gmail account. She reported that the hacker posted "offensive, sexually
16 degrading and disturbing" messages. Ms. Amaral stated that when she was able to access her
17 Gmail account she received a warning that her account had been accessed by IP address
18 98.238.175.73.

19 Victoria Terry provided Ms. Amaral with a copy of images recovered from the folder
20 located within the "nextfornav" folder that was associated with Ms. Amaral. Ms. Amaral
21 confirmed that these were her photos.

22 Stephanie Slevin

23 Victoria Terry related that she received a response from Stephanie Slevin. Stephanie Slevin
24 reported an unknown unauthorized user locked her out of her email accounts @gmail.com, on
25 September 2, 2010. Ms. Slevin advised she was also locked out of her Facebook account and the
26 intruder posted nude photos on her Facebook account that were taken from her Gmail account.

27 _____
28 ⁵ This is the IP address assigned to 5811 Our Way, Citrus Heights, CA

1 She reported that the hacker posted "lewd comments" on her friends Facebook walls while he was
2 in control of her account.

3 Victoria Terry provided Ms. Slevin with a copy of images recovered from the folder located
4 within the "nextfornav" folder that was associated with Ms. Slevin. Ms. Slevin confirmed that
5 these were her photos.

6 Lindsie Ferreira

7 Victoria Terry related that she received a response from Lindsie Ferreira. Ms. Ferreira
8 reported an unknown unauthorized user locked her out of her email accounts @yahoo.com, on
9 July 4, 2010. Ms. Ferreira advised she was also locked out of her Facebook account and the
10 intruder posted nude photos on her Facebook account that were taken from her Gmail account.

11 Victoria Terry provided Ms. Ferreira with a copy of images recovered from the folder
12 located within the "nextfornav" folder that was associated with Ms. Ferreira. Ms. Ferreira
13 confirmed that these were her photos.

14 Laura Kutzler

15 Victoria Terry related that she received a response from Laura Kutzler. Ms. Kutzler
16 reported an unknown unauthorized user accessed her email account @yahoo.com, around the end
17 of February or early March 2010. Ms. Ferreira advised that the intruder accessed her Facebook
18 account and posted "risqué" photos that were taken from her yahoo account.

19 Victoria Terry provided Ms. Ferreira with a copy of images recovered from the folder
20 located within the "nextfornav" folder that was associated with Ms. Ferreira. Ms. Ferreira
21 confirmed that these were her photos.

22 Daniel Piscak

23 Victoria Terry related that she received a response from Daniel Piscak. Ms. Piscak reported
24 an unknown unauthorized user accessed her email account @yahoo.com, during June 2010. Ms.
25 Piscak advised that the intruder also accessed her Facebook account and posted nude photos on
26 her Facebook account that were taken from her yahoo account.

1 Ms. Piscak stated that while she was looking at her hacked Facebook account from a second
2 account that the hacker instant messaged her. When she asked why he was doing this, the hacker
3 replied "because it was funny."

4 Victoria Terry provided Ms. Piscak with a copy of images recovered from the folder
5 located within the "nextfornav" folder that was associated with Ms. Piscak. Ms. Piscak
6 confirmed that these were her photos.

7 Lauren Rackley

8 Victoria Terry related that she received a response from Lauren Rackley. Ms. Rackley
9 reported an unknown unauthorized user accessed her email account @yahoo.com, on four
10 different days: September 27, 2009, March 31, 2010, April 2, 2010, and April 6, 2010. Ms.
11 Rackley advised that the intruder also accessed her Facebook account and posted nude photos on
12 her Facebook account that were taken from her yahoo account. The intruder also emailed the
13 nude photo to everyone on Mr. Rackley's e-mail contact list. Within the "nextfornav" folder, the
14 victim's folder contained nude photographs dated March 31, 2010.⁶

15 Lauren Joyce

16 Victoria Terry related that she received a response from Lauren Joyce. Ms. Joyce reported
17 an unknown unauthorized user accessed her email account @yahoo.com and @gmail.com on
18 December 2, 2009. Ms. Joyce advised that the intruder also accessed her Facebook account and
19 posted nude photos on her Facebook account that she had previously e-mailed to her boyfriend.
20 Within the "nextfornav" folder, the victim's folder contained nude photographs dated December
21 3, 2010.⁷

22 Olivia Chrzanowski

23 Victoria Terry related that she received a response from Olivia Chrzanowski. Ms.
24 Chrzanowski reported an unknown unauthorized user locked her out of her email accounts
25 @gmail.com, during March or April, 2010. Ms. Chrzanowski advised she was also locked out of
26

27 ⁶ This date reflects the date the file was last modified or saved on the hard drive.

28 ⁷ This date reflects the date the file was last modified or saved on the hard drive.

1 her Facebook account and the intruder posted private explicit photos on her Facebook account
2 that were taken from her Gmail account.

3 Victoria Terry provided Ms. Chrzanowski with a copy of images recovered from the folder
4 located within the "nextfornav" folder that was associated with Ms. Chrzanowski. Ms.
5 Chrzanowski confirmed that these were her photos.

6 Kylie Birkicht

7 Victoria Terry related that she received a response from Kylie Birkicht. Ms. Birkicht
8 reported an unknown unauthorized user locked her out of her email account @hotmail.com on
9 August 15, 2010. Ms. Birkicht advised she was also locked out of her Facebook account on
10 August 17, 2010. The intruder posted nude photos on her Facebook account that she had
11 previously deleted from her hotmail account. These nude photos were subsequently posted on
12 other internet photo sites without her permission.

13 Victoria Terry provided Ms. Birkicht with a copy of images recovered from the folder
14 located within the "nextfornav" folder that was associated with Ms. Birkicht. Ms. Birkicht
15 confirmed that these were her photos.

16 Melanie Conway

17 Victoria Terry related that she received a response from Melanie Conway. Ms. Conway
18 reported an unknown unauthorized user locked her out of her email account @gmail.com on
19 April 13, 2010. Ms. Conway advised she was also locked out of her Facebook account and that
20 the intruder posted nude photos on her Facebook account that she had previously sent to her
21 boyfriend. While on her Facebook page, the intruder exchanged messages with other people and
22 released her cellular phone number.

23 Victoria Terry provided Ms. Conway with a copy of images recovered from the folder
24 located within the "nextfornav" folder that was associated with Ms. Conway. Ms. Conway
25 confirmed that these were her photos.

1 Lauren Merino

2 Victoria Terry related that she received a response from Lauren Merino. Ms. Merino
3 reported an unknown unauthorized user locked her out of her email account @yahoo.com, during
4 the summer of 2010. Ms. Merino advised that the intruder also accessed her Facebook account
5 and posted risqué photos on her Facebook account that were taken from her yahoo account. The
6 intruder also posted “racist, crude comments” on other Facebook pages using Ms. Merino’s
7 Facebook account.

8 Ms. Merino provided Victoria Terry with one of the pictures that was taken. Using this
9 sample, Victoria Terry was able to confirm that the photos recovered from the folder located
10 within the “nextfornav” folder that was associated with Ms. Merino.

11 Nora Campbell

12 Victoria Terry related that she received a response from Nora Campbell. Ms. Campbell
13 reported an unknown unauthorized user locked her out of her email account @gmail.com, on July
14 23 and 24th of 2010. Ms. Campbell advised that the intruder accessed a personal erotic video and
15 sent it to everyone on Ms. Campbell’s email contact list under the subject “college” and the text
16 read “watch and enjoy!” The intruder sent the same video to Ms. Campbell’s father from her
17 account with a message reading “Enjoy Dad – love you.” Ms. Campbell reported that she was
18 humiliated.

19 Victoria Terry provided Ms. Campbell with a copy of images recovered from the folder
20 located within the “nextfornav” folder that was associated with Ms. Campbell. Ms. Conway
21 confirmed that these were her photos. An erotic video was also recovered from this “nextfornav”
22 folder that matched the description provided to Victoria Terry by Ms. Campbell.

23 Jane Doe

24 While conducting the forensic analysis, within the the “nextfornav” folder I located a text
25 file in one of the victims’ folders named “*****suicide”⁸ The text file appeared to be a

26
27 ⁸ The folder name has been partially redacted. Since the folder name is the e-mail address
28 of the victim this redaction was done in order to protect the confidential personal information of
the above victim. (See generally Pen. Code, §§ 293.5 and 964)

1 saved online chat session between the account name "*****suicide" and another chat name,
2 "xogreeneyesx3." The text within the file appears to have been saved after some online
3 conversation had passed, but the essence of the conversation indicates the person controlling the
4 user name "xogreeneyesx3" is extorting the female utilizing user name "*****suicide" into
5 taking nude photographs. The user "xogreeneyesx3" claimed to have nude photographs of
6 "*****suicide" and threatened to send the already acquired photographs to email addresses
7 in her contact list. After "*****suicide" pleads with the user controlling account
8 "xogreeneyesx3" to stop the illicit request, the user controlling the account "xogreeneyesx3"
9 attempts to bargain with her advising they can forgo several of the photographs in exchange for
10 recording a video capturing her masturbating. Eventually, "*****suicide" takes
11 photographs and requests a destination.⁹ The user controlling the account "xogreeneyesx3"
12 requests she send the photographs to an email address identified as y*****@gmail.com.

13 At the conclusion of the transfer of photographs, "xogreeneyesx3" agrees to answer
14 questions, to which "*****suicide" asks how her account was accessed. The person
15 controlling the user name "xogreeneyesx3" advises they found her on Facebook, harvested
16 information from her page, as well as her other contacts' pages, then used that information to
17 locate her email account and access the security question.

18
19
20 ⁹ Within the chat "*****suicide" describes her feelings in taking the photographs:
21 04:30] *****suicide: no but im about to keep taking them. i feel fucking raped. i was
already crying from loneliness before you started stuff.

22 ///

23 [04:35] *****suicide: considering there are so many wonderful porn sites and so
many willing females. why did you ahve to take them by force?

24 [04:35] *****suicide: you fucking rapist.

25 [04:35] xogreeneyesx3: i don't quite know. you're attractive enough, but that wasn't the
point. i guess i was seeing how someone would react

26 [04:35] xogreeneyesx3: and that title fits me

27 [04:35] *****suicide: youve actually raped someone?

28 [04:36] xogreeneyesx3: no no no, but i meant it describes what i did to you

[04:36] *****suicide: yeah. you did.

[04:36] *****suicide: i hope youd.

[04:36] *****suicide: you die.

[04:36] xogreeneyesx3: sometimes i hope that too

1 The text file of the chat contains a time log stamp. The chat started at 03:42 and ended at
2 04:43

3 Within the "nextfornav" folder, the victims' folders named "*****suicide" contained
4 12 photographs dated June 5, 2010. Seven of the photographs bear a time modified stamp of 3:03
5 AM to 3:06 AM. The remaining photographs bear a time modified stamp between 3:59 AM and
6 4:45 AM. The last photograph in time depicts a photograph of a young woman masturbating.

7 Within the pass.txt file, I searched for the possible account names of: xogreeneyesx3,
8 "*****suicide" and y*****@gmail.com. I located entries for all three account names,
9 which included date and information line. Based on the conversation between "xogreeneyesx3"
10 and "*****suicide", and the information contained in the pass.txt file, I believe the
11 information line attached to each entry is the answer to the security question for each account Mr.
12 Bronk accessed. Additionally, I noticed all three account entries were located near each other in
13 the file.

14 Based on this online conversation, the emotionally detached messages from the person
15 controlling the user account "xogreeneyesx3," the method described to access the account of
16 "*****suicide," the account used to receive the photographs and the information contained
17 within the pass.txt file, I believe Mr. Bronk gained unauthorized access to the account
18 yaoisama@gmail.com, then illegally accessed the account "xogreeneyesx3." Having control of
19 both of those accounts, he then illegally accessed the account "*****suicide," and searched
20 the account for photographs. Upon locating and downloading photographs from the account, he
21 contacted the user at "*****suicide" via an online chat session, using the account
22 "xogreeneyesx3," then extorted "*****suicide" for further photographs and video.

23 On October 15, 2010, I sent a search warrant to Microsoft for email addresses I extracted
24 from Mr. Bronk's desktop computer. The warrant requested log file information recording IP
25 address 98.238.175.73¹⁰ connecting to the various Microsoft based accounts. One of the email
26 addresses requested was for the email address associated with "*****suicide".

27 _____
28 ¹⁰ This is the IP address assigned to 5811 Our Way, Citrus Heights, CA

1 On October 21, 2010, I received a return from Microsoft, confirming on June 5, 2010, at
2 0302 hours, IP address 98.238.175.73 connected to the account for "*****suicide.

3 **Child Pornography**

4 During the forensic analysis of the evidence items I located a folder on Item #2 at
5 C:\Documents and Settings\Geeg\My Documents\SNES\New Folder which contained a large
6 amount of child pornography images and videos. The images were categorized by folders for
7 each victim, with several victims having multiple folders. The analysis of HDD is still in
8 progress, but as of the writing of this arrest warrant, over 700 child pornography images have
9 been recovered and 15 child pornography videos. It is expected further child pornography will be
10 recovered as the analysis of this item progresses.

11 One of the child pornography videos located in the New Folder, on Mr. Bronk's computer,
12 was labeled "*2yo ass fuck she cries for mommy nasty pthc pedo 1yo 3yo 4yo.mpg*."¹¹

13 Based on the previously stated facts, I believe George Samuel Bronk accessed without
14 authorization e-mail and Facebook accounts and published private information taken from the
15 victim's e-mail accounts on the victims Facebook account. Bronk also extorted nude photographs
16 from a victim by threatening to release photographs in his possession. Finally, Bronk
17 downloaded a large amount of child pornography photographs and videos, then saved the files to
18 his desktop computer.

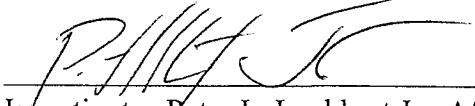
19 These acts are in violation of Penal Code sections 502(c)(1) (computer access and fraud);
20 529 (impersonation of another person); 520 (extortion); and 311.11(a) (possession of child
21 pornography).

22 Therefore, I request that a warrant be issued for the relevant violations charged in the
23 accompanying Complaint.

24
25
26
27 ¹¹ This file is 2 minutes and 18 seconds in length and the focus of the video is primarily on
28 the genitals of a young female child under the age of 18. The video contains an adult male
forcibly inserting his penis into the female child's anus from several angles.

1 I declare under the penalty of perjury under the laws of the State of California that the
2 forgoing is true and correct.

3 Executed on this 28th day of October, 2010, at Sacramento, California.

4
5 
6 Investigator Peter L. Lockhart Jr., Affiant
7 California Highway Patrol
8
9

10 SA2010303587
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28