

United States District Court

FOR THE  
NORTHERN DISTRICT OF CALIFORNIA

VENUE: SAN FRANCISCO

FILED  
2017 FEB 28 P 1:50  
SUSAN Y. SOONG  
CLERK, US DISTRICT COURT  
NO. DIST. OF CA.

UNITED STATES OF AMERICA,

v.

SEALED  
BY COURT ORDER

DMITRY DOKUCHAEV, a/k/a "Patrick  
Nagel," IGOR SUSHCHIN, ALEXSEY  
BELAN, a/k/a "Magg," and KARIM  
BARATOV, a/k/a "Kay," a/k/a "Karim  
Taloverov," a/k/a "Karim Akehmet  
Tokbergenov"

VC

CR17 - 108

DEFENDANT(S).

INDICTMENT

18 U.S.C. § 1030(b) – Conspiracy To Commit Computer Fraud And Abuse; 18 U.S.C. § 1831(a)(5) – Conspiracy To Commit Economic Espionage; 18 U.S.C. § 1832(a)(5) – Conspiracy to Steal Trade Secrets; 18 U.S.C. § 1831(a)(1) – Economic Espionage; 18 U.S.C. § 1832(a)(1) – Theft of Trade Secrets; 18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud; 18 U.S.C. § 1030(a)(2)(C) – Unauthorized Access to Protected Computers; 18 U.S.C. § 1030(a)(5)(A) – Damaging Protected Computers; 18 U.S.C. § 1029(b)(2) – Conspiracy to Commit Fraud in Connection with Access Devices; 18 U.S.C. § 1030(a)(2)(C) – Unauthorized Access to Protected Computers; 18 U.S.C. § 1029(a)(1) – Trafficking in Counterfeit Access Devices; 18 U.S.C. § 1028A – Aggravated Identity Theft; 18 U.S.C. § § 982(a)(2)(B) & 1030(i) and (j) – First Forfeiture Allegation; 18 U.S.C. § § 1834 and 2323 – Second Forfeiture Allegation; 18 U.S.C. § § 981(a)(1)(C), 982(a)(2)(B) and 1029(c)(1)(C) and 28 U.S.C. § 2461(c) – Third Forfeiture Allegation.

A true bill.

[Redacted signature]

Foreman

Filed in open court this 28<sup>th</sup> day of

Feb, 2017

[Handwritten signature]

Clerk

[Handwritten signature]

Bail, \$ no bond for all defendants

Laurel Beeler  
United States Magistrate Judge

1 BRIAN J. STRETCH (CABN 163973)  
2 United States Attorney

FILED  
2017 FEB 28 P 1:50  
SUSAN Y. SOONG  
CLERK, US DISTRICT COURT  
NO. DIST. OF CA.

SEALED  
BY COURT ORDER

8 UNITED STATES DISTRICT COURT  
9 NORTHERN DISTRICT OF CALIFORNIA

VC

10 SAN FRANCISCO DIVISION

11 UNITED STATES OF AMERICA,

**CR 17 103**

12 Plaintiff,

UNDER SEAL

13 v.

VIOLATIONS:

14 DMITRY DOKUCHAEV,  
15 a/k/a "Patrick Nagel"

16 IGOR SUSHCHIN,  
17 ALEXSEY BELAN,  
18 a/k/a "Magg"

19 and  
20 KARIM BARATOV  
21 a/k/a "Kay"

22 a/k/a "Karim Taloverov"  
23 a/k/a "Karim Akehmets Tokbergenov"

24 Defendants.

18 U.S.C. § 1030(b) – Conspiracy To Commit  
Computer Fraud And Abuse; 18 U.S.C. § 1831(a)(5)  
– Conspiracy To Commit Economic Espionage; 18  
U.S.C. § 1832(a)(5) – Conspiracy to Steal Trade  
Secrets; 18 U.S.C. § 1831(a)(1) – Economic  
Espionage; 18 U.S.C. § 1832(a)(1) – Theft of Trade  
Secrets; 18 U.S.C. § 1349 – Conspiracy to Commit  
Wire Fraud; 18 U.S.C. § 1030(a)(2)(C) –  
Unauthorized Access to Protected Computers; 18  
U.S.C. § 1030(a)(5)(A) – Damaging Protected  
Computers; 18 U.S.C. § 1029(b)(2) – Conspiracy to  
Commit Fraud in Connection with Access Devices;  
18 U.S.C. § 1030(a)(2)(C) – Unauthorized Access to  
Protected Computers; 18 U.S.C. § 1029(a)(1) –  
Trafficking in Counterfeit Access Devices; 18 U.S.C.  
§ 1028A – Aggravated Identity Theft; 18 U.S.C. § §  
982(a)(2)(B) & 1030(i) and (j) – First Forfeiture  
Allegation; 18 U.S.C. § § 1834 and 2323 – Second  
Forfeiture Allegation; 18 U.S.C. § § 981(a)(1)(C),  
982(a)(2)(B) and 1029(c)(1)(C) and 28 U.S.C. §  
2461(c) – Third Forfeiture Allegation

25 INDICTMENT

26 The Grand Jury charges—

27 At all times relevant to this Indictment, unless otherwise stated:  
28

INTRODUCTION

1  
2           1.       From at least in or about 2014 up to and including at least in or about December 2016,  
3 officers of the Russian Federal Security Service (“FSB”), an intelligence and law enforcement agency of  
4 the Russian Federation (“Russia”) headquartered in Lubyanka Square, Moscow, Russia, and a successor  
5 service to the Soviet Union’s Committee of State Security (“KGB”), conspired together and with each  
6 other to protect, direct, facilitate, and pay criminal hackers to collect information through computer  
7 intrusions in the United States and elsewhere. The FSB officers, defendants DMITRY DOKUCHAEV,  
8 IGOR SUSHCHIN, and others known and unknown to the Grand Jury, directed the criminal hackers,  
9 defendants ALEXSEY BELAN, KARIM BARATOV, and others known and unknown to the Grand  
10 Jury (collectively, the “conspirators”), to gain unauthorized access to the computers of companies  
11 providing webmail and internet-related services located in the Northern District of California and  
12 elsewhere, to maintain unauthorized access to those computers, and to steal information from those  
13 computers, including information regarding, and communications of, the providers’ users.

14           2.       In some cases, the conspirators sought unauthorized access to information of predictable  
15 interest to the FSB. For example, as described in more detail below, the conspirators sought access to  
16 the Yahoo, Inc. (“Yahoo”) email accounts of Russian journalists; Russian and U.S. government  
17 officials; employees of a prominent Russian cybersecurity company; and numerous employees of U.S.,  
18 Russian, and other foreign webmail and internet-related service providers whose networks the  
19 conspirators sought to further exploit.

20           3.       In other cases, the conspirators sought access to accounts of employees of commercial  
21 entities, including executives and other managers of a prominent Russian investment banking firm (the  
22 “Russian Financial Firm”); a French transportation company; U.S. financial services and private equity  
23 firms; a Swiss bitcoin wallet and banking firm; and a U.S. airline.

24           4.       One of the criminal hackers, BELAN, has been the subject of an Interpol “Red Notice”  
25 and listed as one of the Federal Bureau of Investigation’s (“FBI”) “Most Wanted” hackers since 2012.  
26 BELAN resides in Russia, within the FSB’s jurisdiction to arrest and prosecute. Rather than arrest him,  
27 however, the FSB officers used him. They also provided him with sensitive FSB law enforcement and  
28 intelligence information that would have helped him avoid detection by law enforcement, including

1 information regarding FSB investigations of computer hacking and FSB techniques for identifying  
2 criminal hackers. It was BELAN who provided his FSB conspirators, including DOKUCHAEV and  
3 SUSHCHIN, with the unauthorized access to Yahoo's network described above.

4 5. In addition to executing DOKUCHAEV and SUSHCHIN's taskings, BELAN leveraged  
5 his access to Yahoo's network to enrich himself: (a) through an online marketing scheme, by  
6 manipulating Yahoo search results for erectile dysfunction drugs; (b) by searching Yahoo user email  
7 accounts for credit card and gift card account numbers and other information that could be monetized;  
8 and (c) by gaining unauthorized access to the accounts of more than 30 million Yahoo users, the  
9 contacts of whom were then stolen as part of a spam marketing scheme.

10 6. When the FSB officers, SUSHCHIN and DOKUCHAEV, learned that a target of interest  
11 had email accounts at webmail providers other than Yahoo, including through information gained from  
12 the Yahoo intrusion, they would task BARATOV to access the target's account at the other providers.  
13 When BARATOV was successful, as was often the case, his handling FSB officer, DOKUCHAEV, paid  
14 him a bounty.

15 7. For example, SUSHCHIN, DOKUCHAEV, and BARATOV sought access to the  
16 Google, Inc. ("Google") webmail accounts of:

- 17 a. an assistant to the Deputy Chairman of the Russian Federation;
- 18 b. an officer of the Russian Ministry of Internal Affairs;
- 19 c. a physical training expert working in the Ministry of Sports of a Russian republic; and
- 20 d. others, including additional examples described below.

#### 21 THE DEFENDANTS

22 8. DMITRY ALEKSANDROVICH DOKUCHAEV, also known as "Patrick Nagel," was a  
23 Russian national and resident. DOKUCHAEV was an FSB officer assigned to Second Division of FSB  
24 Center 18, also known as the FSB Center for Information Security. He was an associate of FSB officer  
25 IGOR SUSHCHIN; another, supervisory FSB officer known to the Grand Jury ("FSB Officer 3"), who  
26 was the senior FSB official assigned to Center 18; and other FSB officers known and unknown.  
27 DOKUCHAEV's photograph is attached as Exhibit A.

1           9.       IGOR ANATOLYEVICH SUSHCHIN was a Russian national and resident.  
2 SUSHCHIN was an FSB officer, and DOKUCHAEV's superior within the FSB. SUSHCHIN was also  
3 an associate of FSB Officer 3, and other FSB officers known and unknown. SUSHCHIN was embedded  
4 as a purported employee and Head of Information Security at the Russian Financial Firm, where he  
5 monitored the communications of Russian Financial Firm employees, although it is unknown to the  
6 grand jury whether the Russian Financial Firm knew of his FSB affiliation. SUSHCHIN's photograph is  
7 attached as Exhibit B.

8           10.       ALEXSEY ALEXSEYEVICH BELAN, also known as "Magg," was a Russian national  
9 and resident. He was a criminal hacker and associate of DOKUCHAEV. BELAN assisted  
10 DOKUCHAEV by carrying out hacking assignments. BELAN was indicted in September 2012 in the  
11 District of Nevada for computer fraud and abuse and related crimes in connection with his intrusion into  
12 the computer systems of a U.S. e-commerce company. He was also indicted in June 2013 in the  
13 Northern District of California for computer fraud and abuse and related crimes in connection with  
14 intrusions at two other U.S. e-commerce companies. He was arrested in 2013 in a European country on  
15 a U.S. provisional arrest warrant, but before he could be extradited to the United States, he was able to  
16 leave that country and return to Russia. Currently, BELAN is the subject of an outstanding Interpol  
17 "Red Notice" requesting that Interpol member nations (including Russia) arrest and extradite him.  
18 BELAN is also on the FBI's list of "Most Wanted" hackers and was recently the subject of the  
19 December 29, 2016 sanctions designation by the President of the United States based, at least in part, on  
20 his "significant malicious cyber-enabled misappropriation of personal identifiers for private financial  
21 gain" in relation to the above-described criminal charges. BELAN's photograph is attached as Exhibit  
22 C.

23           11.       KARIM BARATOV, also known as "Kay," "Karim Taloverov" and "Karim Akehm  
24 Tokbergenov," was a Canadian national and resident. He was a criminal hacker and associate of  
25 DOKUCHAEV. BARATOV assisted DOKUCHAEV by carrying out his hacking assignments.  
26 BARATOV's photograph is attached as Exhibit D.

1 COUNT ONE: 18 U.S.C. § 1030(b) – Conspiracy to Commit Computer Fraud and Abuse

2 12. Paragraphs 1 through 11 of this Indictment are hereby re-alleged and incorporated by  
3 reference as if set forth in full herein.

4 13. From a date unknown to the Grand Jury, but no later than January 2014, and continuing  
5 through December 1, 2016, in the Northern District of California and elsewhere, the defendants

6 DMITRY DOKUCHAEV,  
7 ALEXSEY BELAN,  
8 IGOR SUSHCHIN, and  
9 KARIM BARATOV,

10 did knowingly and willfully conspire and agree with each other, and with others known and unknown to  
11 the Grand Jury, to commit computer fraud and abuse, namely:

- 12 a. to access computers without authorization and exceed authorized access to computers, in  
13 the Northern District of California and elsewhere, and to thereby obtain information from  
14 protected computers, for the purpose of commercial advantage and private financial gain,  
15 and in furtherance of a criminal and tortious act in violation of the laws of California,  
16 including invasion of privacy, and where the value of the information did, and would if  
17 completed, exceed \$5,000, in violation of Title 18, United States Code, Sections  
18 1030(a)(2)(C) and 1030(c)(2)(B)(i)-(iii); and
- 19 b. to cause the transmission of programs, information, codes, and commands, in the  
20 Northern District of California and elsewhere, and as a result of such conduct, to cause  
21 damage without authorization to protected computers, and where the offense did cause  
22 and would, if completed, have caused, loss aggregating \$5,000 in value to at least one  
23 person during a one-year period from a related course of conduct affecting a protected  
24 computer, and damage affecting at least 10 protected computers during a one-year period,  
25 in violation of 18 U.S.C. §§ 1030(a)(5)(A) and 1030(c)(4)(B).

26 MANNER AND MEANS OF THE CONSPIRACY

27 14. The conspirators used the following manner and means to accomplish their objectives.

28 15. The conspirators, directly and through intermediaries, attempted to hide the nature and  
origin of their internet traffic and reduce the likelihood of detection by victims and law enforcement, by

1 leasing servers in numerous countries, including the United States, and using other services like virtual  
2 private networks.

3 16. The conspirators used numerous email accounts hosted by webmail providers in the  
4 United States and elsewhere, including Russia, which they often registered using false subscriber  
5 information.

6 17. In some instances, the conspirators used email messages known as “spear phishing”  
7 messages to trick unwilling recipients into giving the co-conspirators access to their computers and  
8 accounts. Spear phishing messages typically were designed to resemble emails from trustworthy  
9 senders, and to encourage the recipient to open attached files or click on hyperlinks in the messages.  
10 Some spear phishing emails attached or linked to files that, once opened or downloaded, installed  
11 “malware”—malicious code or programs—that provided unauthorized access to the recipient’s  
12 computer (a “backdoor”). Other spear phishing emails lured the recipient into providing valid login  
13 credentials to his or her account(s), thereby allowing the defendants to bypass normal authentication  
14 procedures.

15 18. In many instances, the conspirators engaged in the manual creation of account  
16 authentication “cookies,” known as “minting,” to gain unauthorized access to victim webmail accounts.  
17 Cookies are small files stored on a user’s computer by the user’s web browser. Upon a user’s  
18 connection to a webmail server, the server can read the data in the cookie and obtain information about  
19 that specific user. Among other uses, cookies enable webmail providers to recognize an account user  
20 who had previously logged into his or her account, and to allow that user, for a specified duration, to  
21 continue to access the account’s contents without re-entering his or her password.

22 19. The conspirators frequently sought unauthorized access to the email accounts of close  
23 associates of their intended victims, including spouses and children, to gain additional information about  
24 and belonging to their intended victims.

1                   The Yahoo Intrusions

2           20.     Yahoo was a webmail provider based in Sunnyvale, California, which provided internet  
3 services, including electronic messaging services, to more than 1 billion users.

4           21.     Beginning no later than 2014, the conspirators stole non-content information regarding  
5 more than 500 million Yahoo user accounts as a result of their malicious intrusion. The theft of user  
6 data was part of a larger intrusion into Yahoo's computer network, which continued to and including at  
7 least September 2016. As part of this intrusion, malicious files and software tools were downloaded  
8 onto Yahoo's computer network, and used to gain and maintain further unauthorized access to Yahoo's  
9 network and to conceal the extent of such access.

10          22.     The user data referenced in the preceding paragraph was held in Yahoo's User Database  
11 ("UDB"). The UDB was, and contained, proprietary and confidential Yahoo technology and  
12 information, including, among other data, subscriber information, such as: account users' names;  
13 recovery email accounts and phone numbers, which users provide to webmail providers, such as Yahoo,  
14 as alternative means of communication with the provider; password challenge questions and answers;  
15 and certain cryptographic security information associated with the account, *i.e.* the account's "nonce",  
16 further described below. Some of the information in the UDB was stored in an encrypted form.

17          23.     Yahoo used its Account Management Tool ("AMT") to access and edit the information  
18 stored in the UDB. The AMT allowed Yahoo to manage aspects of its users' accounts, including to  
19 make, log, and track changes to the account, such as password changes. The AMT was, and contained,  
20 proprietary and confidential Yahoo technology and information.

21          24.     In or around early 2014, the conspirators gained unauthorized access to Yahoo's network  
22 and began their reconnaissance. After gaining unauthorized access to Yahoo's network, BELAN  
23 located relevant Yahoo network resources of interest, including the UDB and AMT.

24          25.     In or around November and December 2014, BELAN stole a backup copy of the UDB as  
25 it existed in early November 2014. He removed at least some of the UDB copy to one of the computers  
26 under his control (the "BELAN Computer") by using the File Transfer Protocol, a common means of  
27 transferring data between computers.



1           26.     Beginning in or around October 2014 and until at least November 2016, the conspirators  
2 accessed user account information and contents using a combination of methods, including without  
3 limitation: (a) via unauthorized access to Yahoo’s AMT; (b) via the minting of authentication cookies on  
4 Yahoo’s network to gain unauthorized access to victim webmail accounts; and (c) via the minting of  
5 authentication cookies outside Yahoo’s network.

6           27.     The conspirators minted authentication cookies “internally”, *i.e.* within Yahoo’s network,  
7 while they trespassed on the network. In order to mint cookies internally, the conspirators caused  
8 programs to be loaded onto Yahoo’s network and computers without authorization.

9           28.     The conspirators also minted authentication cookies “externally”, *i.e.* outside Yahoo’s  
10 network. In order to mint cookies externally, the conspirators required, among other information, a  
11 cryptographic value unique to the targeted victim account, called a “nonce.” The nonces associated with  
12 individual Yahoo user accounts were stored in the UDB, and thus when BELAN stole a copy of at least  
13 a portion of the UDB in November and December 2014, the defendants obtained the nonces associated  
14 with affected user accounts.

15           29.     Whenever a Yahoo user changed his or her password, the nonce associated with the  
16 account changed as well. As a result, comparing the date that victims last changed their passwords to  
17 the defendants’ cookie minting attempts confirms that the conspirators employed the UDB copy that  
18 BELAN stole—*i.e.*, the UDB as it existed in early November 2014—to gain unauthorized access to  
19 Yahoo user accounts via external cookie minting. The conspirators failed to access those accounts  
20 whose users had changed their passwords after BELAN stole the UDB copy; but they succeeded in  
21 accessing those accounts that retained the same passwords in use at the time the conspirators obtained  
22 the UDB copy, including those accounts for which the user had most recently changed the password  
23 immediately prior to BELAN’s theft of the UDB copy.

24           30.     The conspirators discussed among themselves how to mint cookies to access Yahoo  
25 accounts. For example, on or about July 20, 2015, DOKUCHAEV sent SUSHCHIN a minted cookie for  
26  
27  
28

1 a Yahoo user account, a file containing the below screenshot of a cookie manager application, and  
2 instructions for using the application to access the Yahoo email account.

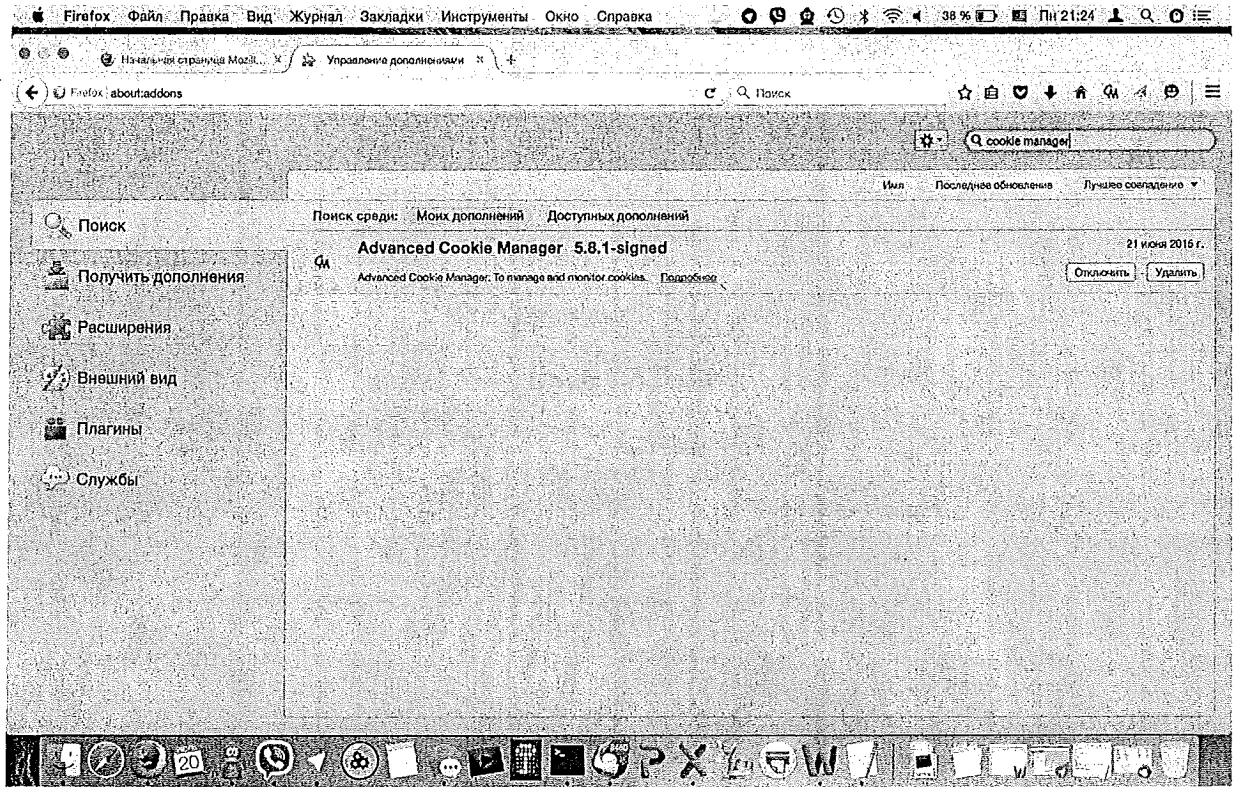


Figure 1: Screenshot of a cookie manager application

17 31. Both internally and externally minted cookies allowed the conspirators to appear to  
18 Yahoo's servers as if the intruder had previously obtained valid access to the associated Yahoo user's  
19 account, obviating the need to enter a username and password for that account. The conspirators utilized  
20 cookie minting to access the contents of more than 6,500 Yahoo user accounts.

21 32. The conspirators used their access to the AMT to (among other unauthorized actions)  
22 maintain persistent unauthorized access to some of the compromised accounts.

23 33. The AMT did not permit text searches of underlying data. It permitted the conspirators to  
24 access information about particular Yahoo user accounts. However, by combining their control of the  
25 stolen UDB copy and access to the AMT, the conspirators could, for example, search the UDB contents  
26 to identify Yahoo user accounts for which the user had provided a recovery email account hosted by a  
27 specific company of interest to the conspirators (e.g., "exampleuser@ExampleCompany.com")—  
28 showing that the user was likely an employee of the company of interest—and then use information

1 from the AMT to gain unauthorized access to the identified accounts using the means described in  
2 paragraph 26.

3 34. The conspirators used their unauthorized access to Yahoo's network to identify and  
4 access accounts of, among other victims, users affiliated with U.S. online service providers, including  
5 but not limited to webmail providers and cloud computing companies, whose account contents could  
6 facilitate unauthorized access to other victim accounts; Russian journalists and politicians critical of the  
7 Russian government; Russian citizens and government officials; former officials from countries  
8 bordering Russia; and U.S. government officials, including cyber security, diplomatic, military, and  
9 White House personnel. For example:

- 10 a. In or around October 2014, the conspirators sought, and DOKUCHAEV later obtained,  
11 access to an account of a diplomat from a country bordering Russia who was posted in a  
12 European country.
- 13 b. From at least in or around December 2015 until May 2016, the conspirators sought access  
14 to accounts of the former Minister of Economic Development of a country bordering  
15 Russia ("Victim A") and his wife ("Victim B"). DOKUCHAEV, SUSHCHIN, and  
16 BELAN worked with FSB Officer 3 to access Victims A and B's accounts by minting  
17 cookies and to share information obtained from those accounts. In one instance, on or  
18 about December 18, 2015, FSB Officer 3 provided SUSHCHIN with information  
19 regarding a company controlled by Victims A and B. On or about December 21, 2015,  
20 DOKUCHAEV sent a cookie for Victim B's account to SUSHCHIN, who then later that  
21 day sent DOKUCHAEV a report on Victims A and B. On or about May 20, 2016,  
22 BELAN minted a cookie for the same Victim B account.
- 23 c. In or around December 2015 and January 2016, the conspirators sought access to an  
24 account of a Russian journalist and investigative reporter who worked for Kommersant  
25 Daily. DOKUCHAEV obtained information about the victim's account from the AMT  
26 and then obtained full access to the victim user's account by minting cookies on or about  
27 December 6, 2015, and January 21, 2016.
- 28

- 1 d. In or around December 2015 and January 2016, the conspirators sought access to an  
2 account of a public affairs consultant and researcher who analyzed Russia's bid for  
3 World Trade Organization membership. DOKUCHAEV accessed the contents of the  
4 victim user's account by minting cookies.
- 5 e. In or around February 2016, the conspirators sought access to Yahoo accounts of  
6 employees of a U.S. cloud storage company's ("U.S. Cloud Computing Company 1").  
7 On or about February 26, 2016, DOKUCHAEV gained accessed to the Yahoo user  
8 accounts of three different officers of U.S. Cloud Computing Company 1, in each case by  
9 minting cookies.
- 10 f. In or around March 2016, the conspirators sought access to an account of a Russian  
11 Deputy Consul General. On or about March 19, 2016, DOKUCHAEV successfully  
12 minted a cookie to gain access to the victim's account.
- 13 g. In or around April 2016, the conspirators sought access to an account of a senior officer  
14 at a Russian webmail and internet-related services provider (the "Russian Webmail  
15 Provider"). On or about April 25, 2016, DOKUCHAEV successfully minted a cookie to  
16 gain access to the victim user's account.

17 35. The conspirators used their unauthorized access to Yahoo's network in order to defraud  
18 Yahoo users as well. For a period in or around November 2014, at around the same time he was  
19 working to provide DOKUCHAEV and SUSHCHIN with access to Yahoo's network, BELAN  
20 manipulated some of the servers associated with Yahoo's English-language search engine so that when  
21 users searched for erectile dysfunction medications, they were presented with a fraudulent link created  
22 by BELAN. When a Yahoo user clicked on that link, he or she was taken to the website of a U.S.-based  
23 cloud computing firm, U.S. Cloud Computing Company 2. The Yahoo search engine users were then  
24 automatically redirected, by malicious code placed by BELAN on the website of U.S. Cloud Computing  
25 Company 2, and without themselves taking any additional actions, to the website of an online pharmacy  
26 company. That online pharmacy company's marketing program paid commissions to marketers who  
27 successfully drove traffic to its website. As a result, BELAN was paid for diverting Yahoo search  
28 engine users to it.

1           36.    Other examples of Yahoo users whose accounts the conspirators targeted and  
2 compromised include:

- 3           a.    On or about July 11, 2015, BELAN gained access to accounts belonging to 14 employees  
4           of a Swiss bitcoin wallet and banking firm.
- 5           b.    On or about February 13, 2016, one conspirator gained access to an account belonging to  
6           a sales manager at a major U.S. financial company.
- 7           c.    On or about March 30, 2016, DOKUCHAEV gained access to an account belonging to a  
8           Nevada gaming official.
- 9           d.    On or about April 14, 2016, BELAN gained access to an account belonging to a senior  
10          officer of a major U.S. airline.
- 11          e.    On or about June 20, 2016, a defendant gained access to an account belonging to a  
12          Shanghai-based managing director of a U.S. private equity firm.
- 13          f.    On or about October 22, 2016, the conspirators gained access to accounts of the Chief  
14          Technology Officer of a French transportation company.
- 15          g.    The conspirators sought access to accounts of multiple Yahoo users affiliated with the  
16          Russian Financial Firm. In one instance, in or around April 2015, SUSHCHIN ordered  
17          DOKUCHAEV to target a number of individuals, including a senior board member of the  
18          Russian Financial Firm, his wife, and his secretary; and a senior officer of the Russian  
19          Financial Firm (“Corporate Officer 1”). In or around April 2015, the conspirators gained  
20          access to a Yahoo account the conspirators mistakenly believed belonged to Corporate  
21          Officer 1. In or around October 2015, SUSHCHIN and DOKUCHAEV then developed a  
22          spear phishing email to send to Corporate Officer 1, purporting to originate from the  
23          Russian Federal Tax Service, in an attempt to gain unauthorized access to another non-  
24          Yahoo email account the officer controlled. The targeting of the Russian Financial Firm  
25          continued into 2016. Specifically, on or about January 13, 2016, the conspirators used  
26          Yahoo’s AMT to access data associated with the account of the above-referenced board  
27          member’s secretary.
- 28

1           37. BELAN also stole financial information from certain Yahoo user accounts for personal  
2 gain. For example, on or about April 26, 2015, BELAN searched within a victim user's account for  
3 credit card verification values ("cvv" numbers). As another example, on or about June 20, 2015, he did  
4 the same within a different user account, in addition to searching for "amex"; then he moved to another  
5 victim account and searched for, among other terms, "visa," "amex," "mastercard," and "credit . . .  
6 card"; then searched for those same terms in yet another user's account on the same day. In all, BELAN  
7 sought financial information from at least eight Yahoo users' accounts that day.

8           38. BELAN sought to steal gift card information from victim email accounts as well. For  
9 example, on or about October 8, 2016, BELAN searched the email accounts of at least 15 Yahoo victim  
10 users for gift cards, including by searching for the email address from which a major U.S. online retailer  
11 sent gift cards to its customers.

12           39. In addition, BELAN used his access to Yahoo's network to further a spam marketing  
13 scheme by minting cookies that enabled access to more than 30 million victim user accounts. From at  
14 least in or around March 2015 until in or around July 2015, BELAN used a malicious script he placed on  
15 Yahoo's network to mint cookies in bulk (up to at least tens of thousands of cookies at a time). Using  
16 computers under his control, including the BELAN Computer, BELAN minted in bulk cookies that were  
17 later used to steal the email contacts of the victim accounts; such contacts are valuable to spammers  
18 because they permit spammers to send emails purporting to originate from associates or acquaintances  
19 of targeted recipients, making it more likely the targeted recipient will open the spam email. Thousands  
20 of the bulk-minted cookies were removed from Yahoo's network to the BELAN Computer.

21           40. As they victimized Yahoo, the conspirators took steps to conceal their actions from  
22 Yahoo and law enforcement. For example, BELAN downloaded to Yahoo's network from the BELAN  
23 Computer a program known as a "log cleaner." This program sought to remove traces of the intrusion  
24 from Yahoo's records (logs) of network activity, to make the conspirators more difficult to track.

25           41. Finally, the conspirators used the stolen Yahoo data to compromise related user accounts  
26 at Yahoo, Google, and other webmail providers, including the Russian Webmail Provider. Among other  
27 means, they exploited the Yahoo data by searching within victim user accounts for other Yahoo or non-  
28 Yahoo accounts controlled by the same victim that the conspirators could later target for unauthorized

1 access; passwords; challenge question answers; and other information of use to the conspirators. For  
2 example:

- 3 a. On or about August 31, 2015, BELAN gained access to a Yahoo user account, then  
4 searched for terms including “password” and “Google” and phrases including “Google . .  
5 . account,” “Apple . . . account,” and “itunes . . . account.”
- 6 b. On or about September 29, 2015, BELAN gained access to a Yahoo user account  
7 controlled by an officer of a U.S.-based technology and internet-related services company  
8 (the “U.S. Technology Company”) and then searched that account for terms and phrases  
9 including “[U.S. Technology Company]” . . . password,” “VPN,” and “[Yahoo user  
10 name]@[U.S. Technology Company].com.”

#### 11 The Google and Other Account Intrusions

12 42. During the same period that DOKUCHAEV, SUSHCHIN, and BELAN were committing  
13 intrusions into the Yahoo computer network and the accounts of individual Yahoo users,  
14 DOKUCHAEV and SUSHCHIN were directing BARATOV to access individual accounts provided by  
15 Google, the Russian Webmail Provider, and other webmail providers. For example, the conspirators  
16 sought unauthorized access to the accounts of:

- 17 a. An assistant to the Deputy Chairman of the Russian Federation;
- 18 b. A managing director, a former sales officer, and a researcher, all of whom worked for a  
19 major Russian cyber security firm;
- 20 c. An officer of the Russian Ministry of Internal Affairs assigned to that Ministry’s  
21 “Department K,” its “Bureau of Special Technical Projects,” which investigates cyber,  
22 high technology, and child pornography crimes;
- 23 d. A physical training expert working in the Ministry of Sports of a Russian republic; and
- 24 e. A Russian official who was both Chairman of a Russian Federation Council committee  
25 and a senior official at a major Russian transport corporation.

26 43. In some cases, DOKUCHAEV and SUSHCHIN identified target accounts based on  
27 information obtained through unauthorized access to Yahoo’s network and its users’ accounts. For  
28 example, on or about October 9, 2014, the conspirators accessed records for account

1 \*\*\*\*\*as@yahoo.com in the AMT, associated with the CEO of a metals industry holding company in a  
2 country bordering Russia. Using the AMT, they changed the Yahoo user's recovery email account to an  
3 account controlled by DOKUCHAEV; then, approximately five minutes later, DOKUCHAEV falsely  
4 verified the change by clicking on an email link automatically generated by Yahoo. DOKUCHAEV  
5 then changed the account password. The next day, on or about October 10, 2014, DOKUCHAEV asked  
6 BARATOV to gain access to \*\*\*\*\*as@gmail.com, the account that had served as  
7 \*\*\*\*\*as@yahoo.com's recovery email account until DOKUCHAEV's change the day before.

8 44. Also on or about October 9, 2014, DOKUCHAEV sought unauthorized access to account  
9 \*\*\*\*\*ov@yahoo.com, belonging to a prominent banker and university trustee in a country bordering  
10 Russia. DOKUCHAEV changed the recovery account to one DOKUCHAEV controlled and changed  
11 the victim account password. Then, on or about October 10, 2014, DOKUCHAEV tasked BARATOV  
12 with gaining unauthorized access to \*\*\*\*\*ov@gmail.com, the account that had served as  
13 \*\*\*\*\*ov@yahoo.com's recovery email account until DOKUCHAEV's change the day before.

14 45. In other instances, the conspirators used their unauthorized access to Yahoo's network to  
15 obtain additional information about individuals who controlled accounts at other webmail providers to  
16 which the conspirators sought unauthorized access. For example,

17 a. On or about February 25, 2016, the conspirators gained unauthorized access to  
18 information in the AMT regarding a Yahoo account belonging to an International  
19 Monetary Fund official. One week later, on or about March 2, 2016, the conspirators  
20 gained access to that account by minting a cookie. That same day, the conspirators  
21 searched within that Yahoo user account for a particular Google account belonging to a  
22 managing director of a finance and banking company in a country bordering Russia.  
23 Then, on or about March 24, 2016, DOKUCHAEV tasked BARATOV with gaining  
24 unauthorized access to that Google account.

25 b. In another example, on or about March 2, 2016, the conspirators searched a Yahoo  
26 account belonging to an advisor to a senior official in a country bordering Russia, for  
27 "\*\*\*\*\*va@gmail.com," an email account belonging to a prominent business  
28 woman from that country. Then, on or about March 24, 2016, DOKUCHAEV tasked



1 BARATOV with gaining access to the same, searched-for Google account,  
2 \*\*\*\*\*va@gmail.com.

3 46. SUSHCHIN also identified accounts to target that were associated with the Russian  
4 Financial Firm. For example, in or around April 2015, SUSHCHIN sent DOKUCHAEV a list of email  
5 accounts associated with Russian Financial Firm personnel and family members to target, including  
6 Google accounts. During these April 2015 communications, SUSHCHIN identified a Russian Financial  
7 Firm employee to DOKUCHAEV as the “main target.” Also during these April 2015 communications,  
8 SUSHCHIN forwarded to DOKUCHAEV an email sent by that “main target’s” wife to a number of  
9 other Russian Financial Firm employees. SUSHCHIN added the cover note “this may be of some use.”  
10 In another example, between in or about December 2015 and May 2016, SUSHCHIN directed  
11 DOKUCHAEV, who in turn directed BARATOV, to obtain unauthorized access to the Google and other  
12 accounts of Victims A and B and their family (discussed in paragraph 34.b above).

13 47. During the conspiracy DOKUCHAEV tasked BARATOV with obtaining unauthorized  
14 access to at least 80 identified email accounts, including at least 50 identified Google accounts.

15 48. BARATOV knowingly and with intent to defraud sought unauthorized access to Google  
16 and other accounts on behalf of DOKUCHAEV and SUSHCHIN through techniques such as spear  
17 phishing. He created and maintained multiple email accounts for the purpose of sending spear phishing  
18 emails to victims that he targeted at DOKUCHAEV and SUSHCHIN’s behest.

19 49. When BARATOV successfully obtained unauthorized access to a victim’s account, he  
20 notified DOKUCHAEV and provided evidence of that access. He then demanded payment—generally  
21 approximately U.S. \$100—via online payment services.

22 50. Once DOKUCHAEV sent BARATOV a payment, BARATOV provided DOKUCHAEV  
23 with valid, illicitly obtained account credentials permitting DOKUCHAEV, SUSHCHIN, and others  
24 known and unknown to thereafter access the victim’s account without further assistance from  
25 BARATOV.

26 All in violation of Title 18, United States Code, Section 1030(b).  
27  
28

1 COUNT TWO: 18 U.S.C. § 1831(a)(5) – Conspiracy to Engage in Economic Espionage

2 51. Paragraphs 1 through 11 and 14 through 50 of this Indictment are hereby re-alleged and  
3 incorporated by reference as if set forth in full herein.

4 52. In connection with the management and protection of its user accounts, Yahoo developed  
5 and maintained proprietary technology that constituted trade secrets as defined in Title 18, United States  
6 Code, Section 1839(3), including:

- 7 a. Yahoo's UDB and the data therein, including user data such as the names of Yahoo users,  
8 identified recovery email accounts and password challenge answers, and Yahoo-created  
9 and controlled data regarding its users' accounts;
- 10 b. Yahoo's AMT, its method and manner of functioning and capabilities, and the data it  
11 contained and provided; and
- 12 c. Yahoo's cookie minting source code.

13 53. From at least in or about January 2014, until December 1, 2016, in the Northern District  
14 of California and elsewhere, the defendants,

15 DMITRY DOKUCHAEV,  
16 IGOR SUSHCHIN, and  
ALEXSEY BELAN,

17 together with others known and unknown to the Grand Jury, knowingly combined, conspired, and  
18 agreed to:

- 19 a. Knowingly and without authorization steal, appropriate, take, and by fraud, artifice, and  
20 deception obtain trade secrets belonging to Yahoo;
- 21 b. Knowingly and without authorization copy, duplicate, alter, replicate, transmit, deliver,  
22 send, communicate, and convey trade secrets belonging to Yahoo; and
- 23 c. Knowingly receive, buy, and possess trade secrets belonging to Yahoo, knowing the  
24 same to have been stolen, appropriated, obtained, and converted without authorization;  
25 intending and knowing that the offenses would benefit a foreign government, namely Russia, and a  
26 foreign instrumentality, namely the FSB, in violation of Title 18, United States Code, Section  
27 1831(a)(1), (2), and (3).
- 28

1           54.    In furtherance of the conspiracy and to effect its objects, DOKUCHAEV, SUSHCHIN,  
2 and BELAN committed the following acts:

- 3           a.    In or about October 2014, DOKUCHAEV accessed records for user accounts in Yahoo's  
4            AMT.
- 5           b.    On or about November 10, 2014, BELAN stole the Yahoo UDB by removing at least a  
6            portion of it to the BELAN Computer.
- 7           c.    On or about December 12, 2014, DOKUCHAEV minted an unauthorized cookie.
- 8           d.    On or about July 16, 2015, BELAN minted in bulk cookies permitting access to at least  
9            17,000 Yahoo user accounts.
- 10          e.    On or about July 20, 2015, DOKUCHAEV instructed SUSHCHIN how to use minted  
11          cookies to access Yahoo user accounts.
- 12          f.    On or about December 21, 2015, DOKUCHAEV minted a cookie for a Yahoo user  
13          account and then sent the minted cookie to SUSHCHIN.
- 14          g.    On or about January 13, 2016, the conspirators accessed Yahoo's AMT to obtain  
15          unauthorized access to data associated with a Yahoo user account.
- 16          h.    On or about March 25, 2016, BELAN used a minted cookie to gain access to a Yahoo  
17          user's account.
- 18          i.    On or about May 5, 2016, DOKUCHAEV sent a minted cookie for a Yahoo user's  
19          account to SUSHCHIN.
- 20          j.    On or about May 10, 2016, SUSHCHIN sent DOKUCHAEV screen shots of victim  
21          accounts, including a Yahoo user's account, to which SUSHCHIN had gained  
22          unauthorized access.
- 23          k.    On or about July 25, 2016, DOKUCHAEV sent BELAN information regarding FSB law  
24          enforcement and intelligence investigations, and FSB tactics, including its use of  
25          informants to target hackers whose difficult-to-trace computer intrusion infrastructure  
26          made other means of surveillance more difficult.

27           All in violation of Title 18, United States Code, Section 1831(a)(5).  
28

1 COUNT THREE: 18 U.S.C. § 1832(a)(5) – Conspiracy to Commit Theft of Trade Secrets

2 55. Paragraphs 1 through 11, 14 through 50, 52, and 54 of this Indictment are hereby re-  
3 alleged and incorporated by reference as if set forth in full herein.

4 56. From at least in or about January 2014, until December 1, 2016, in the  
5 Northern District of California and elsewhere, the defendants,

6 DMITRY DOKUCHAEV,  
7 IGOR SUSHCHIN, and  
8 ALEXSEY BELAN,

9 together with others known and unknown to the Grand Jury, knowingly combined, conspired, and  
10 agreed to:

- 11 a. Knowingly and without authorization steal, appropriate, take, and by fraud, artifice, and  
12 deception obtain trade secrets belonging to Yahoo that were related to a product or  
13 service used in and intended to be used in interstate and foreign commerce;
- 14 b. Knowingly and without authorization copy, duplicate, alter, replicate, transmit, deliver,  
15 send, communicate, and convey trade secrets belonging to Yahoo that were related to a  
16 product or service used in and intended to be used in interstate and foreign commerce;  
17 and
- 18 c. Knowingly receive, buy, and possess trade secrets belonging to Yahoo that were related  
19 to a product or service used in and intended to be used in interstate and foreign  
20 commerce, knowing the same to have been stolen, appropriated, obtained, and converted  
21 without authorization;

22 intending to convert those trade secrets to the economic benefit of someone other than Yahoo, and  
23 intending and knowing that the offense would injure Yahoo, in violation of Title 18, United States Code,  
24 Section 1832(a)(1), (2), and (3).

25 57. In furtherance of the conspiracy and to effect its objects, conspirators committed the overt  
26 acts alleged in paragraph 54.

27 All in violation of Title 18, United States Code, Section 1832(a)(5).  
28

1 COUNTS FOUR THROUGH SIX: 18 U.S.C. § 1831(a)(1) and (4) – Economic Espionage

2 58. Paragraphs 1 through 11, 14 through 50, 52, and 54 of this Indictment are hereby re-  
3 alleged and incorporated by reference as if set forth in full herein.

4 59. In or about the dates set forth below, in the Northern District of California and  
5 elsewhere, the defendants,

6 DMITRY DOKUCHAEV,  
7 IGOR SUSHCHIN, and  
8 ALEXSEY BELAN,

9 knowingly stole and without authorization appropriated, took, and concealed, and by fraud, artifice, and  
10 deception obtained a trade secret belonging to Yahoo, and attempted to do so, intending and knowing  
11 that the offense would benefit a foreign government, specifically Russia, and a foreign instrumentality,  
12 specifically the FSB.

COUNT	IN OR ABOUT	NATURE OF ECONOMIC ESPIONAGE
FOUR	November-December 2014	Theft of at least a portion of Yahoo's UDB
FIVE	October 2014-March 2016	Theft of information regarding the functioning of the Yahoo AMT
SIX	August 2015	Theft of Yahoo cookie minting source code

15 All in violation of Title 18, United States Code, Sections 1831(a)(1) and (4), and 2.

16  
17 COUNT SEVEN THROUGH NINE: 18 U.S.C. § 1832(a)(1) – Theft of Trade Secrets

18 60. Paragraphs 1 through 11, 14 through 50, 52, and 54 of this Indictment are hereby re-  
19 alleged and incorporated by reference as if set forth in full herein.

20 61. In or about the dates set forth below, in the Northern District of California and  
21 elsewhere, the defendants,

22 DMITRY DOKUCHAEV  
23 ALEXSEY BELAN, and  
24 IGOR SUSHCHIN,

25 knowingly stole and without authorization appropriated, took, and concealed, and by fraud, artifice, and  
26 deception obtained, a trade secret belonging to Yahoo, and attempted to do so, which was related to a  
27 product or service used in and intended to be used in interstate and foreign commerce, intending to  
28 convert that trade secret to the economic benefit of someone other than Yahoo, and intending and

1 knowing that the offense would injure Yahoo.

COUNT	IN OR ABOUT	TRADE SECRET THEFT
SEVEN	November-December 2014	Theft of at least a portion of Yahoo's UDB
EIGHT	October 2014-March 2016	Theft of information regarding the functioning of the Yahoo AMT
NINE	August 2015	Theft of Yahoo cookie minting source code

5 All in violation of Title 18, United States Code, Sections 1832(a)(1) and 2.

7 COUNT TEN: 18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud

8 62. Paragraphs 1 through 11, 14 through 50, and 54 of this Indictment are hereby re-alleged  
9 and incorporated by reference as if set forth in full herein.

10 63. From at least in or about January 2014, until December 1, 2016, in the Northern District  
11 of California and elsewhere, the defendants,

12 DMITRY DOKUCHAEV,  
13 IGOR SUSHCHIN and  
ALEXSEY BELAN,

14 together with others known and unknown to the Grand Jury, conspired to devise a scheme and artifice to  
15 defraud and to obtain property from Yahoo and Yahoo users by means of materially false and fraudulent  
16 pretenses, representations, and promises, and did knowingly transmit and cause to be transmitted by  
17 means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures, and  
18 sounds, namely transmitting malicious computer code, illicitly obtained credentials, and fraudulent  
19 messages, for the purpose of executing and attempting to execute the scheme and artifice.

20 64. Specifically, DOKUCHAEV, SUSHCHIN, and BELAN conspired to devise a scheme  
21 whereby BELAN gained unauthorized access to Yahoo's network, among other means by stealing and  
22 employing Yahoo employee credentials. It was further part of the scheme that BELAN provided access  
23 to Yahoo's network to DOKUCHAEV and SUSHCHIN who, with BELAN, stole, created, and  
24 employed account credentials, including minted authentication cookies, to obtain unauthorized access to  
25 Yahoo data and user accounts.

26 65. DOKUCHAEV, SUSHCHIN, and BELAN thereby fraudulently obtained property from  
27 Yahoo and Yahoo users' accounts, including among other items, non-public information of value to  
28 each of the conspirators; gift card numbers redeemable at online merchants; access to payment accounts

1 such as PayPal and Western Union accounts; information about credit card cvv numbers; and the  
2 contacts of Yahoo users.

3 66. In furtherance of the scheme to defraud, BELAN also manipulated Yahoo search engine  
4 code for personal financial gain.

5 All in violation of Title 18, United States Code, Section 1349.

6 COUNTS ELEVEN THROUGH THIRTEEN: 18 U.S.C. § 1030(a)(2)(C) – Unauthorized Access to  
7 Protected Computers

8 67. Paragraphs 1 through 11, 14 through 50, and 54 of this Indictment are hereby re-alleged  
9 and incorporated by reference as if set forth in full herein.

10 68. On or about the dates set forth below, in the Northern District of California and  
11 elsewhere, the defendants

12 DMITRY DOKUCHAEV,  
13 IGOR SUSHCHIN, and  
14 ALEXSEY BELAN,

15 intentionally and without authorization attempted to access and did access a protected computer  
16 belonging to Yahoo, and thereby obtained information for commercial advantage and private financial  
17 gain; obtained information in furtherance of criminal and tortious acts in violation of the laws of  
18 California, including invasion of privacy; and obtained information valued in excess of \$5,000.

COUNT	ON OR ABOUT	NATURE OF ACCESS
ELEVEN	September 2014	Accessing and scanning of Yahoo's corporate network from a Yahoo server and the theft of information regarding Yahoo's network architecture.
TWELVE	November 10, 2014	Accessing of Yahoo's corporate network and the theft of at least a portion of Yahoo's UDB.
THIRTEEN	December 12, 2014	Accessing of Yahoo's corporate network and theft of at least a portion of Yahoo's UDB.

19  
20  
21  
22  
23 All in violation of Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(i)-(iii),  
24 and 2.

1 COUNTS FOURTEEN THROUGH SEVENTEEN: 18 U.S.C. § 1030(a)(5)(A) –Damaging  
2 Protected Computers

3 69. Paragraphs 1 through 11, 14 through 50, and 54 of this Indictment are hereby re-alleged  
4 and incorporated by reference as if set forth in full herein.

5 70. On or about the dates set forth below, in the Northern District of California and  
6 elsewhere, the defendants

7 DMITRY DOKUCHAEV  
8 IGOR SUSHCHIN, and  
9 ALEXSEY BELAN,

10 knowingly attempted to cause and did cause the transmission of a program, information, code, and  
11 command, and as a result of such conduct, would and did intentionally cause damage without  
12 authorization to at least ten protected computers during a one-year period and causing more than \$5,000  
13 in loss in one year.

COUNT	ON OR ABOUT	DAMAGING ACT
FOURTEEN	October 30, 2014	Placement of malicious code on Yahoo's network to provide a means of facilitating the conspirators' future access to Yahoo's servers
FIFTEEN	November 10, 2014	Modification of code on Yahoo's system to direct certain Yahoo search engine users to an online pharmacy
SIXTEEN	June 8, 2015 through July 16, 2015	Placement of a malicious script onto Yahoo's network to internally mint cookies. The results of this script (cookies that would allow access to victims' accounts) were then exfiltrated
SEVENTEEN	August 13, 2015	Placement of a new script used to internally mint cookies onto Yahoo's network

19  
20 All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B), and 2.  
21  
22  
23  
24  
25  
26  
27  
28



1 COUNTS EIGHTEEN THROUGH TWENTY-FOUR: 18 U.S.C. § 1030(a)(2)(C) – Unauthorized  
2 Access to Protected Computers

3 71. Paragraphs 1 through 11, 14 through 50, and 54 of this Indictment are hereby re-alleged  
4 and incorporated by reference as if set forth in full herein.

5 72. On or about the dates set forth below, in the Northern District of California and  
6 elsewhere, the defendants

7 DMITRY DOKUCHAEV,  
8 IGOR SUSHCHIN, and  
9 ALEXSEY BELAN,

10 intentionally and without authorization attempted to access and did access a protected computer  
11 belonging to Yahoo, and thereby obtained and attempted to obtain information for commercial  
12 advantage and private financial gain; information in furtherance of criminal and tortious acts in violation  
of the laws of California, including invasion of privacy; and information valued in excess of \$5,000.

COUNT	ON OR ABOUT	NATURE OF ACCESS
EIGHTEEN	April 16, 2016	BELAN accessed *****35@yahoo.com using a fraudulently minted cookie.
NINETEEN	February 26, 2016	DOKUCHAEV accessed ****ey@yahoo.com using a fraudulently minted cookie.
TWENTY	March 30, 2016	DOKUCHAEV accessed ****re4@yahoo.com using a fraudulently minted cookie.
TWENTY-ONE	May 17, 2016	BELAN accessed *****tter@yahoo.com using a fraudulently minted cookie.
TWENTY-TWO	May 18, 2016	BELAN accessed *****35@yahoo.com using a fraudulently minted cookie.
TWENTY-THREE	March 30, 2016	DOKUCHAEV accessed *****feld@yahoo.com using a fraudulently minted cookie.
TWENTY-FOUR	March 30, 2016	DOKUCHAEV accessed *****rosa@yahoo.com using a fraudulently minted cookie.

21  
22 All in violation of Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(i)-(iii),  
23 and 2.

24 COUNTS TWENTY-FIVE THROUGH THIRTY-SIX: 18 U.S.C. § 1029(a)(1) – Counterfeit Access  
25 Devices

26 73. Paragraphs 1 through 11, 14 through 50, and 54 of this Indictment are hereby re-alleged  
27 and incorporated by reference as if set forth in full herein.

1 74. On or about the dates set forth below, in the Northern District of California and  
2 elsewhere, the defendants,

3 DMITRY DOKUCHAEV,  
4 IGOR SUSHCHIN, and  
ALEXSEY BELAN,

5 did knowingly and with intent to defraud, produce, use, and traffic in at least one counterfeit access  
6 device, and attempted to do so.

COUNT	ON OR ABOUT	COUNTERFEIT ACCESS DEVICE
TWENTY-FIVE	July 16, 2015	BELAN minted at least 17,000 cookies.
TWENTY-SIX	July 20, 2015	DOKUCHAEV sent SUSHCHIN a minted cookie for ***tech@yahoo.com.
TWENTY-SEVEN	September 9, 2015	DOKUCHAEV produced and used a minted cookie to gain unauthorized access to account *****30@yahoo.com.
TWENTY-EIGHT	September 29, 2015	BELAN produced and used a minted cookie to gain unauthorized access to account *****on@yahoo.com.
TWENTY-NINE	September 29, 2015	BELAN produced and used a minted cookie to gain unauthorized access to account *****54@yahoo.com.
THIRTY	September 29, 2015	BELAN produced and used a minted cookie to gain unauthorized access to account *****on@yahoo.com.
THIRTY-ONE	September 29, 2015	BELAN produced and used a minted cookie to gain unauthorized access to account *****ey@yahoo.com.
THIRTY-TWO	September 29, 2015	BELAN produced and used a minted cookie to gain unauthorized access to account *****20@yahoo.com.
THIRTY-THREE	December 21, 2015	DOKUCHAEV sent SUSHCHIN a minted cookie for *****08@yahoo.com.
THIRTY-FOUR	April 25, 2016	DOKUCHAEV produced and used a minted cookie to gain unauthorized access to account *****ru@yahoo.com.
THIRTY-FIVE	April 25, 2016	DOKUCHAEV produced and used a minted cookie to gain unauthorized access to account *****ov@yahoo.com.
THIRTY-SIX	May 5, 2016	DOKUCHAEV sent SUSHCHIN a minted cookie for *****08@yahoo.com.

20 All in violation of Title 18, United States Code, Sections 1029(a)(1), 1029(b)(1), and 2.

21  
22 COUNT THIRTY-SEVEN: 18 U.S.C. § 1029(a)(4) – Device Making Equipment

23 75. Paragraphs 1 through 11, 14 through 50, and 54, of this Indictment are hereby re-alleged  
24 and incorporated by reference as if set forth in full herein.

25 76. From in or about December 2015 until in or about March 2016, in the Northern District  
26 of California and elsewhere, the defendants,

27 DMITRY DOKUCHAEV,  
28 IGOR SUSHCHIN, and  
ALEXSEY BELAN,

1 did knowingly and with intent to defraud produce, traffic in, have control and custody of, and possess  
2 device-making equipment, and attempted to do so, to wit, tools and software that could be and were used  
3 to mint unauthorized cookies permitting unauthorized access to Yahoo user accounts, as alleged in  
4 paragraph 74.

5 All in violation of Title 18, United States Code, Sections 1029(a)(4) and 2.

6 COUNT THIRTY-EIGHT: 18 U.S.C. § 1029(b)(2) – Conspiracy to Commit Fraud in  
7 Connection with Access Devices

8 77. Paragraphs 1 through 11, 14 through 50, and 54, and the factual allegations set forth in  
9 paragraph 75 of this Indictment are hereby re-alleged and incorporated by reference as if set forth in full  
10 herein.

11 78. From at least in or about January 2014, until December 1, 2016, in the Northern District  
12 of California and elsewhere, the defendants,

13 DMITRY DOKUCHAEV,  
14 IGOR SUSHCHIN, and  
15 KARIM BARATOV,

16 and others known and unknown, knowingly conspired, combined, and agreed to, and did, with intent to  
17 defraud, in an offense affecting interstate and foreign commerce:

- 18 a. traffic in and use at least one unauthorized access device during a one-year period, to  
19 obtain something of value aggregating at least \$1,000 during that period, in violation of  
20 Title 18, United States Code, Section 1029(a)(2); and  
21 b. effect transactions, with at least one access device issued to another person, to receive  
22 payment and another thing of value during a one-year period, the aggregate value of  
23 which was at least \$1,000, in violation of Title 18, United States Code, Section  
24 1029(a)(5).

25 79. Specifically, BARATOV sought and gained unauthorized access to Google and other  
26 webmail provider accounts as requested by DOKUCHAEV, sometimes after DOKUCHAEV's  
27 discussions with SUSHCHIN. BARATOV provided the means of unauthorized access in the form of  
28 valid, but illicitly obtained passwords, to DOKUCHAEV. DOKUCHAEV then paid BARATOV for  
providing DOKUCHAEV with such information, thereby enabling unauthorized access to the requested

1 email accounts. In total, DOKUCHAEV paid BARATOV money and other things of value aggregating  
2 at least \$1,000 for unauthorized email account access during a one-year period, from April 17, 2015  
3 through April 17, 2016.

4 OVERT ACTS

5 80. In furtherance of the conspiracy and to effect its illegal objects, BARATOV,  
6 DOKUCHAEV, and SUSHCHIN committed the following acts:

- 7 a. On or about October 10, 2014, DOKUCHAEV sent BARATOV a request for  
8 unauthorized access to \*\*\*\*\*as@gmail.com and \*\*\*\*\*ov@gmail.com.
- 9 b. On or about October 10, 2014, DOKUCHAEV sent BARATOV a request for  
10 unauthorized access to more than 30 Google accounts, not including the two described in  
11 the preceding paragraph.
- 12 c. On or about December 26, 2014, BARATOV sent DOKUCHAEV the password for  
13 \*\*\*\*\*17@gmail.com, to which account DOKUCHAEV had tasked BARATOV to  
14 gain unauthorized access.
- 15 d. On or about January 2, 2015, BARATOV sent DOKUCHAEV the password for  
16 \*\*\*\*\*2011@gmail.com, to which account DOKUCHAEV had tasked BARATOV to  
17 gain unauthorized access.
- 18 e. On or about July 6, 2015, BARATOV sent DOKUCHAEV the password for  
19 \*\*\*\*\*77@gmail.com, to which account DOKUCHAEV had tasked BARATOV to gain  
20 unauthorized access.
- 21 f. On or about August 1, 2015, BARATOV sent DOKUCHAEV a second password for  
22 \*\*\*\*\*2011@gmail.com, an account for which BARATOV had sent DOKUCHAEV a  
23 password on or about January 2, 2015, and, to which account DOKUCHAEV had tasked  
24 BARATOV to gain unauthorized access
- 25 g. On or about September 30, 2015, BARATOV sent DOKUCHAEV the password for  
26 \*\*\*\*\*um@gmail.com, to which account DOKUCHAEV had tasked BARATOV to  
27 gain unauthorized access.
- 28

- 1 h. On or about November 16, 2015, DOKUCHAEV sent BARATOV a request for  
2 unauthorized access to \*\*\*\*br@gmail.com and \*\*\*\*ov@gmail.com.
- 3 i. On or about November 17, 2015, BARATOV sent DOKUCHAEV the password for  
4 \*\*\*\*ov@gmail.com, to which account DOKUCHAEV had tasked BARATOV to gain  
5 unauthorized access.
- 6 j. On or about November 17, 2015, DOKUCHAEV paid BARATOV U.S. \$104.20.
- 7 k. On or about December 3, 2015, BARATOV sent DOKUCHAEV the password for  
8 \*\*\*\*13@gmail.com, to which account DOKUCHAEV had tasked BARATOV to  
9 gain unauthorized access.
- 10 l. On or about March 24, 2016, DOKUCHAEV sent BARATOV a request for unauthorized  
11 access to \*\*\*\*\*va@gmail.com.
- 12 m. On or about March 25, 2016, BARATOV sent DOKUCHAEV the password for  
13 \*\*\*\*\*21@gmail.com, to which account DOKUCHAEV had tasked BARATOV to  
14 gain unauthorized access.

15 All in violation of Title 18, United States Code, Sections 1029(b)(2).

16

17 COUNT THIRTY-NINE: 18 U.S.C. § 1349 – Conspiracy to Commit Wire Fraud

18 81. Paragraphs 1 through 11, 14 through 50, 54, and 80, and the factual allegations set forth  
19 in paragraph 74 of this Indictment are hereby re-alleged and incorporated by reference as if set forth in  
20 full herein.

21 82. From at least in or about January 2014, until December 1, 2016, in the Northern District  
22 of California and elsewhere, the defendants,

23 DMITRY DOKUCHAEV,  
24 IGOR SUSHCHIN and  
KARIM BARATOV,

25 together with others known and unknown to the Grand Jury, conspired to devise a scheme and artifice to  
26 defraud and to obtain property from Google account users by means of materially false and fraudulent  
27 pretenses, representations, and promises, and did knowingly transmit and cause to be transmitted by  
28 means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures, and

1 sounds, namely transmitting malicious computer code, illicitly obtained credentials, and fraudulent  
2 messages, for the purpose of executing and attempting to execute the scheme and artifice, in violation of  
3 Title 18, United States Code, Section 1343.

4 83. Specifically, DOKUCHAEV and SUSHCHIN identified email accounts to which they  
5 wanted access. DOKUCHAEV then directed BARATOV to attempt to gain unauthorized access to at  
6 least 80 email accounts, including at least 50 Google accounts. BARATOV attempted to obtain access  
7 credentials for the accounts through "spear phishing." BARATOV, when successful, sent  
8 DOKUCHAEV the passwords for the accounts.

9 84. Upon successfully gaining the credentials for a tasked account, BARATOV informed  
10 DOKUCHAEV that he could be paid for his work in Russian rubles, U.S. dollars, Ukrainian hryvnia, or  
11 Euros through online payment services. DOKUCHAEV then paid BARATOV using these means.

12 All in violation of Title 18, United States Code, Section 1349.

13  
14 COUNTS FORTY THROUGH FORTY-SEVEN: 18 U.S.C. § 1028A(a)(1) – Aggravated Identity Theft

15 85. Paragraphs 1 through 50 and 80 of this Indictment are hereby re-alleged and incorporated  
16 by reference as if set forth in full herein.

17 86. On or about the dates set forth below, in the Northern District of California and  
18 elsewhere, the defendants,

19 **DMITRY DOKUCHAEV and**  
20 **KARIM BARATOV,**

21 during and in relation to the crimes of Conspiracy to Commit Computer Fraud, in violation of 18 U.S.C.  
22 Section 1030(b), Unauthorized Access to Computers, in violation of 18 U.S.C. Section 1030(a)(2),  
23 Conspiracy to Commit Fraud and Related Activity in Connection with Access Devices, in violation of  
24 18 U.S.C. Section 1029(b)(2), and Conspiracy to Commit Wire Fraud, in violation of 18 U.S.C. Section  
25 1349, did knowingly transfer, possess, and use, without lawful authority, the means of identification of  
26 another person.

27

COUNT	ON OR ABOUT	IDENTIFICATION OF ANOTHER PERSON
FORTY	December 26, 2014	BARATOV sent DOKUCHAEV the password and email address for *****17@gmail.com.
FORTY-ONE	January 2, 2015	BARATOV sent DOKUCHAEV the password and email

28

		address for *****2011@gmail.com.	
1	FORTY-TWO	July 6, 2015	BARATOV sent DOKUCHAEV the password and email address for *****77@gmail.com.
2	FORTY-THREE	August 1, 2015	BARATOV sent DOKUCHAEV the password and email address for *****2011@gmail.com.
3	FORTY-FOUR	September 30, 2015	BARATOV sent DOKUCHAEV the password and email address for *****um@gmail.com.
4	FORTY-FIVE	November 17, 2015	BARATOV sent DOKUCHAEV the password and email address for ****ov@gmail.com.
5	FORTY-SIX	December 3, 2015	BARATOV sent DOKUCHAEV the password and email address for *****13@gmail.com.
6	FORTY-SEVEN	March 25, 2016	BARATOV sent DOKUCHAEV the password and email address for *****21@gmail.com.
7			

8 All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2, and Title 28, United  
9 States Code, Section 3238.

10  
11 FIRST FORFEITURE ALLEGATION: 18 U.S.C. § 982(a)(2)(B) & 1030(i) and (j)

12 87. The allegations contained in paragraphs one to eleven and Counts One and Eleven  
13 through Twenty-Four are hereby re-alleged and incorporated by reference for the purpose of alleging  
14 forfeiture pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i) and (j).

15 88. Upon conviction of any of the offenses in violation of Title 18, United States Code,  
16 Section 1030 as set forth in Counts One and Eleven through Twenty-Four of this Indictment, defendants

17 DMITRY DOKUCHAEV,  
18 ALEXSEY BELAN,  
19 IGOR SUSHCHIN, and  
20 KARIM BARATOV,

shall forfeit to the United States of America:

- 21 a. pursuant to Title 18, United States Code, Sections 982(a)(2)(B), any property  
22 constituting, or derived from, proceeds obtained directly or indirectly as a result of said  
23 violations; and  
24 b. pursuant to Title 18, United States Code, Sections 1030(i) and (j), any property  
25 constituting, or derived from, proceeds obtained directly or indirectly as a result of said  
26 violations, and any property used to commit or facilitate the commission of said violation  
27 or conspiracy thereto.

28 89. The property subject to forfeiture shall include, but not be limited to the following:

- a. All funds which constitute proceeds that are held on deposit in PayPal account number xxxxxxxxxxxxxxxx9844, held by BARATOV in the name of "Elite Space Corporation";
- b. All funds which constitute proceeds that are held on deposit in PayPal account number xxxxxxxxxxxxxxxx2639, held by DOKUCHAEV;
- c. a grey Aston Martin DBS, license plate identification "MR KARIM"; and
- d. a black Mercedes Benz C54, license plate identification "CAWE693."

90. If, as a result of any act or omission of the defendants, any of said property:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to or deposited with, a third person;
- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which without difficulty cannot be subdivided;

any and all interest defendants have in any other property (not to exceed the value of the above forfeitable property), including but not limited to a grey Aston Martin DBS, license plate identification "MR KARIM," and a black Mercedes Benz C54, license plate identification "CAWE693," shall be forfeited to the United States, pursuant to Title 21, United States Code, Section 853(p) and as incorporated in Title 28, United States Code, Sections 2323(b).

SECOND FORFEITURE ALLEGATION: 18 U.S.C. § § 1834 and 2323

91. The allegations contained in paragraphs one to eleven and Counts Two through Nine are hereby re-alleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 1834 and 2323.

92. Upon conviction of any of the offenses in violation of Title 18, United States Code, Section 1030 as set forth in Counts Two through Nine of this Indictment, defendants

DMITRY DOKUCHAEV,  
ALEXSEY BELAN, and  
IGOR SUSHCHIN,

shall forfeit to the United States of America, pursuant to Title 18, United States Code, Sections 1834 and 2323, any property used or intended to be used in any manner or part to commit or facilitate the



1 offenses, and any property constituting or derived from the proceeds obtained directly or indirectly as a  
2 result of said offenses.

3 93. The property subject to forfeiture shall include, but not be limited to all funds which  
4 constitute proceeds that are held on deposit in PayPal account number xxxxxxxxxxxxxxxx2639, held by  
5 DOKUCHAEV.

6 94. If, as a result of any act or omission of the defendants, any of said property:

- 7 a. cannot be located upon the exercise of due diligence;
- 8 b. has been transferred or sold to or deposited with, a third person;
- 9 c. has been placed beyond the jurisdiction of the Court;
- 10 d. has been substantially diminished in value; or
- 11 e. has been commingled with other property which without difficulty cannot be subdivided;

12 any and all interest defendants have in any other property (not to exceed the value of the above  
13 forfeitable property), including but not limited to a grey Aston Martin DBS, license plate identification  
14 "MR KARIM," and a black Mercedes Benz C54, license plate identification "CAWE693," shall be  
15 forfeited to the United States, pursuant to Title 21, United States Code, Section 853(p) and as  
16 incorporated in Title 28, United States Code, Sections 2323(b).

17  
18 THIRD FORFEITURE ALLEGATION: 18 U.S.C. § 981(a)(1)(C), 982(a)(2)(B) and 1029(c)(1)(C)  
19 and 28 U.S.C. § 2461(c)

20 95. The allegations contained in paragraphs one to eleven and Counts Ten and Twenty-Five  
21 through Thirty-Eight are hereby re-alleged and incorporated by reference for the purpose of alleging  
22 forfeiture pursuant to Title 18, United States Code, Sections (a)(2)(B) and 1029(c)(1)(C) and Title 28,  
23 United States Code, Section 2461(c).

24 96. Upon conviction of any of the offenses in violation of Title 18, United States Code,  
25 Sections 1029 and 1349 as set forth in Counts Ten and Twenty-Five through Thirty-Eight of this  
26 Indictment, defendants

27  
28  
DMITRY DOKUCHAEV,  
ALEXSEY BELAN,  
IGOR SUSHCHIN, and  
KARIM BARATOV,

1 shall forfeit to the United States of America:

- 2 a. pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States
- 3 Code, Section 2461(c), any property, real or personal, which constitutes or is derived
- 4 from proceeds traceable to these violations;
- 5 b. pursuant to Title 18, United States Code, Section 982(a)(2)(B), any property constituting
- 6 or derived from proceeds obtained directly or indirectly as a result of these violations;
- 7 c. pursuant to Title 18, United States Code, Section 1029(c)(1)(C), any personal property
- 8 used or intended to be used to commit a violation of Title 18, United States Code, Section
- 9 1029.

10 97. The property subject to forfeiture shall include, but not be limited to the following:

- 11 a. All funds which constitute proceeds that are held on deposit in PayPal account number
- 12 xxxxxxxxxxxxxxxx9844 held by BARATOV in the name of "Elite Space Corporation";
- 13 b. All funds which constitute proceeds that are held on deposit in PayPal account number
- 14 xxxxxxxxxxxxxxxx2639, held by DOKUCHAEV;
- 15 c. a grey Aston Martin DBS, license plate identification "MR KARIM"; and
- 16 d. a black Mercedes Benz C54, license plate identification "CAWE693."

17 98. If, as a result of any act or omission of the defendants, any of said property:

- 18 a. cannot be located upon the exercise of due diligence;
- 19 b. has been transferred or sold to or deposited with, a third person;
- 20 c. has been placed beyond the jurisdiction of the Court;
- 21 d. has been substantially diminished in value; or
- 22 e. has been commingled with other property which without difficulty cannot be subdivided;

23 any and all interest defendants have in any other property (not to exceed the value of the above

24 forfeitable property), including but not limited to a grey Aston Martin DBS, license plate identification

25

26

27

28

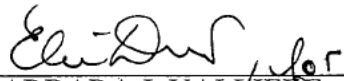
1 "MR KARIM," and a black Mercedes Benz C54, license plate identification "CAWE693," shall be  
2 forfeited to the United States, pursuant to Title 21, United States Code, Section 853(p) and as  
3 incorporated in Title 28, United States Code, Sections 2461(c).

4  
5 DATED: 2/28/17

A TRUE BILL

6  
7   
8 FOREPERSON

9 BRIAN J. STRETCH  
United States Attorney

10   
11 BARBARA J. VALLIERE  
Chief, Criminal Division

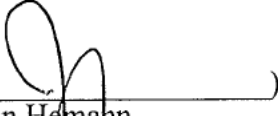
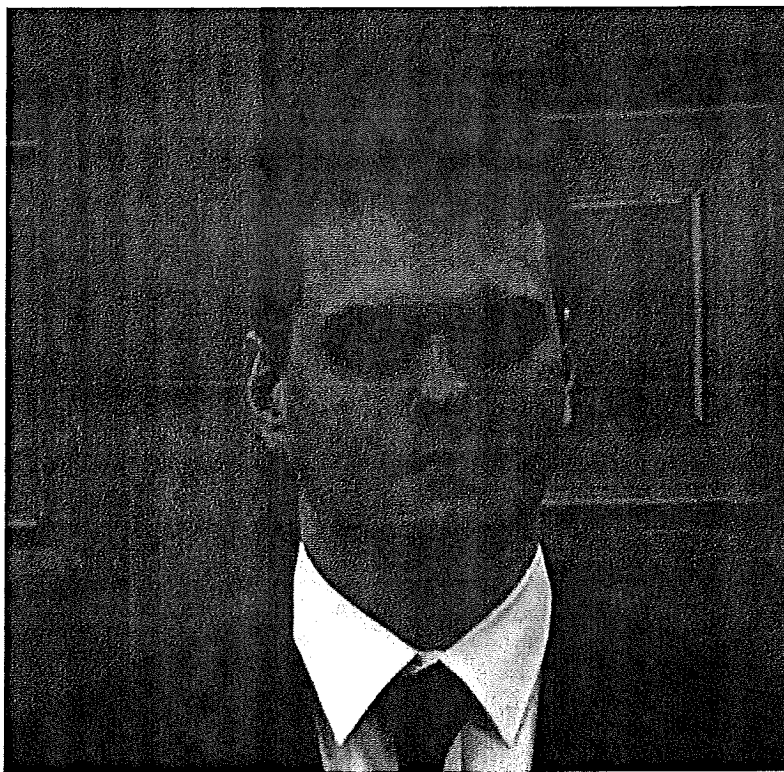
12  
13 (Approved as to form: )  
14 AUSA John Hemann  
NSD Trial Attorney Scott McCulloch  
NSD Cyber Counsel Christopher Ott

Exhibit A



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

Exhibit B



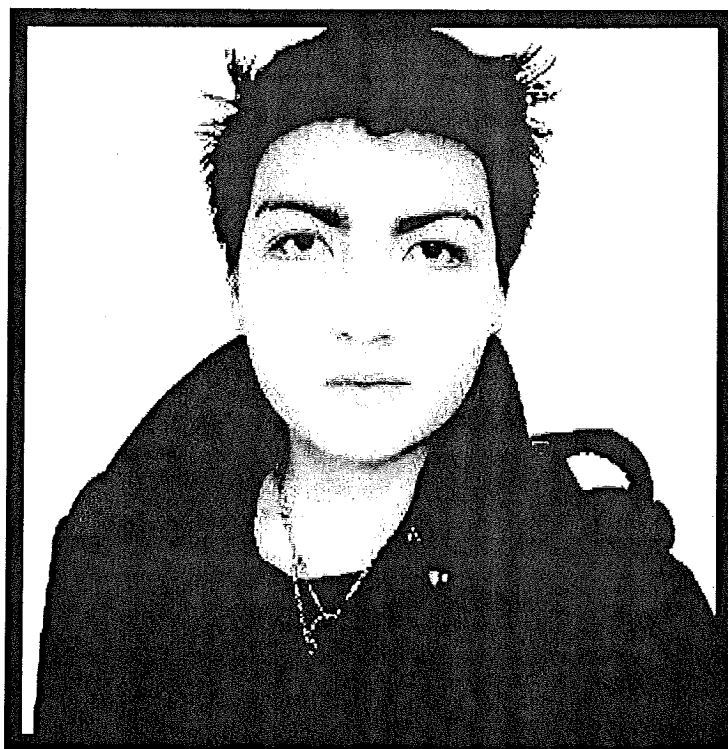
1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Exhibit C



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

Exhibit D



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