DAVID L. ANDERSON (CABN 149604)
United States Attorney

HALLIE HOFFMAN (CABN 210020)
Chief, Criminal Division

MICHELLE J. KANE (CABN 210579)
KATHERINE L. WAWRZYNIAK (CABN 252751)
Assistant United States Attorneys

1301 Clay Street, Suite 340S
Oakland, California 94612
Telephone: (510) 637-3680
FAX: (510) 637-3724
michelle.kane3@usdoj.gov
Katherine.Wawrzyniak@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

| | |
|---|---|
| UNITED STATES OF AMERICA,<br><br>Plaintiff,<br><br>v.<br><br>YEVGENIY ALEXANDROVICH NIKULIN,<br><br>Defendant. | No. CR 16-00440 WHA<br><br>**UNITED STATES' TRIAL BRIEF**<br><br>Trial: March 9, 2020<br>Time: 1:30 p.m.<br>Courtroom No. 12 |

**TABLE OF CONTENTS**

## TABLE OF AUTHORITIES

**Cases**



**Statutes**

**Rules**



**Other Authorities**

The United States of America by and through undersigned counsel, respectfully submits this trial brief for purposes of summarizing the legal and factual issues it believes will be relevant to the upcoming trial, set to begin on March 9, 2020. At the pretrial conference on February 19, 2020, the Court also requested copies of the "top ten" trial exhibits. Those exhibits are being filed as exhibits to this brief, including two videos that were previously discussed with the Court.

## I. SUMMARY OF FACTS TO BE PRESENTED AT TRIAL

### A. Overview

During 2012 and 2013, defendant Yevgeniy Nikulin engaged in a sustained campaign to steal user account credentials from major U.S. companies. Defendant repeatedly targeted employees of the victim corporations that, based on their positions, he knew would have high level access to corporate data. Once he compromised those employees' corporate account credentials, he used their access to obtain millions of consumer user names and passwords, in addition to other information. Those credentials were extremely valuable on the underground market for their use in spamming and other illicit purposes.

### B. The Attack on LinkedIn and its Employees

In March 2012, defendant Yevgeniy Nikulin, operating from Russia, gained access to the personal computer of LinkedIn engineer Nicholas Berry. LinkedIn is a networking site that includes technical and security professionals from major Silicon Valley companies as members. Through his position, Berry had access to core LinkedIn data. Berry owned an Apple iMac computer, which he sometimes used to work from home. He also ran a "virtual machine" on the iMac that acted as a personal web server. Defendant compromised the virtual machine and, through a security flaw, was able to gain access to the iMac itself. In doing so, he installed software on the computer. Because Berry used the iMac to access LinkedIn corporate computers through a Virtual Private Network ("VPN")[1], Nikulin was able to gain access to LinkedIn's servers through Berry's VPN credentials. Once he had access to LinkedIn's servers, Nikulin could obtain a copy of LinkedIn's user credential database. Although the

///

[1] A VPN is often used by businesses so employees can connect to their office network from another location.

passwords in that database were encrypted, the copy that Nikulin gained access to was not yet "salted," which was a stronger form of encryption that LinkedIn was in the process of instituting.

LinkedIn learned of the breach in June 2012 when a portion of the stolen data was posted on a Russian hacker forum with a request for help with decryption. Upon embarking on an internal investigation, LinkedIn security personnel observed suspicious logins from Berry's VPN account from IP addresses that resolved to Russia. After confirming that Berry had not traveled to Russia and was not responsible for those logins, LinkedIn investigated information captured by its VPN and other logs. LinkedIn identified several Russian IP addresses that accessed its computers, indicating that someone in Russia was responsible for the access. Exhibit A (Summary of LinkedIn VPN Logs for User NBerry). LinkedIn also identified other data captured by its logs, including the "user agent string" and "cookie," two pieces of information that help identify a particular computer. [2] This data indicated that the same computer was likely responsible for multiple accesses across different IP addresses. Furthermore, LinkedIn found evidence that the same computer had also accessed multiple LinkedIn consumer accounts. Finally, LinkedIn identified one account, with the username chinabig01@gmail.com that had been accessed from one of the same IP addresses used in the compromise of Nick Berry's VPN credentials. Exhibit B (LinkedIn, Dropbox, and Formspring Emails from chinabig01@gmail.com Account).

The FBI reviewed LinkedIn data and Berry's computer and came to the same conclusion. Due to the access to customer LinkedIn accounts, the FBI contacted the employers of those customers regarding possible attacks on their computer systems. The FBI also began following the leads generated from the LinkedIn investigation, including the chinabig01@gmail.com address.

**C. The Continuing Investigation and Development of Chinabig01@gmail.com**

Following the attack on LinkedIn, Dropbox found numerous unauthorized logins from Eastern European IP addresses on its own system between May and July 2012. Dropbox disclosed those IP

[2] A user agent string is information regarding a user's web browser and computer that is passed to a website in order to display content correctly. The general format for user agent strings is "Mozilla/[version] ([system and browser information]) [platform] ([platform details]) [extensions]." A cookie in this context is a small piece of unique data sent from a website and stored in a user's web browser while the user is browsing a website. When the user browses to the same website in the future, the data stored in the cookie is retrieved by the website to notify it of the user's previous activity.

addresses to the FBI. The FBI also obtained records regarding a Dropbox account that had been registered just before the attack on Dropbox's system with the username chinabig01@gmail.com. IP logs from that account showed that it was accessed from the same IP addresses that accessed Dropbox accounts without authorization.

The FBI thus began focusing on the person controlling chinabig01@gmail.com as the person responsible for the LinkedIn and Dropbox intrusions. A search warrant for that email account revealed an email message indicating that Dropbox employee Tom Wiegand had "invited" the owner of the chinabig01@gmail.com Dropbox account to a Dropbox shared account, when he had not done so. Wiegand's account had been compromised, and the invitation showed that the person controlling chinabig01@gmail.com was responsible. Other evidence from the chinabig01@gmail.com account linking the owner to the attacks included a search for information related to an "SSH key"[3] in February 2012, shortly before the compromise of Nick Berry's computer, which obtained the SSH key used to authenticate his VPN connection.

**D. Subscriber Records Identify Nikulin**

Subscriber records obtained through Russian authorities showed that Nikulin, at an address on Kantemirovskaya Street in Moscow, was the registered subscriber of one of the IP addresses used to access LinkedIn computers without authorization. Exhibit C (National Cable Networks Subscriber Information). That IP address also accessed multiple LinkedIn member accounts between February and April 2012, and was one of the IP addresses linked by cookies to other unauthorized access at LinkedIn.

**E. Nikulin Controls Both Chinabig01@gmail.com and R00talka@gmail.com**

The FBI identified an account with a gaming website, Kongregate that had been accessed by an IP addresses used in the LinkedIn attack, including one that was also used to access the chinabig01@gmail.com Dropbox account. The Kongregate account and the chinabig01@gmail.com Dropbox account both used the name "Jammis" in their subscriber information. The Kongregate account showed a user name of "Zopaqwe1" and was registered under r00talka@mail.ru, which is hosted by a Russian email provider generally unavailable to U.S. authorities. An account with the DNS provider

[3] SSH refers to the "secure shell" protocol that many businesses use to secure the connection between an individual computer or "client" and a server.

Afraid.org using the email address chinabig01@gmail.com also had the password Zopaqwe1. These links all showed that the same person was using the Kongregate, Dropbox, Gmail, and Afraid. org accounts.

The contents of the email account r00talka@gmail.com (similar to the r00talka@mail.ru account used with Kongregate) indicated that it was controlled by the same person controlling chinabig01@gmail.com. For example, multiple messages addressed to "china" or "china china" were found in both accounts and registration confirmations from Russian companies noted the same password, "qwe123!" for accounts registered under both email addresses. Moreover, the contents of the r00talka@gmail.com account pointed directly to Nikulin. These included multiple messages generated through the VK social media platform to the r00talka@gmail.com account, including links to messages from Nikulin's brother and girlfriend. Exhibit D (Translation of VK Email from r00talka@gmail.com Account). The messages from VK often included a photo of Nikulin and a photo of the person sending the message. The search history for the r00talka@gmail.com account showed Nikulin searching for terms including "LinkedIn hack" and "Wordpress vulnerabilities." Exhibit E (Translation of r00talka@gmail.com search history). These links established that Nikulin controlled both the r00talka@gmail.com and chinabig01@gmail.com accounts, and was responsible for the LinkedIn, Dropbox, and Formspring intrusions.

**F. Sale of Formspring Credentials**

Between June 13, 2012, and June 29, 2012, Nikulin stole approximately 30 million Formspring user credentials after compromising the account of a Formspring employee, John Sanders (identified in the Indictment as J.S.). The Formspring logs show that defendant used Sanders' credentials to login to Formspring's servers and execute the attack, including the installation of malicious software. In July 2012, Formspring discovered that a portion of its encrypted password database had been posted online. The IP address used in the Formspring attack was also used to access multiple LinkedIn member accounts.

Nikulin then conspired with several individuals to sell the stolen Formspring credentials. In July 2012, Alexsey Belan, encouraged Nikita Kislitsin to contact Nikulin about the Formspring database. After Kislitsin confirmed that he had contacted Nikulin, Kislitsin and Belan discussed how a brute-force

password cracker, and not Nikulin himself, had posted the encrypted Formspring passwords online. Kislitsin then negotiated the sale of the database in September 2012 to another individual, who paid through Western Union via another individual, Oleg Tolstikh. Kislitsin sent a sample of the data, which Formspring confirms was their user information. Exhibit F (Excerpt of Translation of Email Messages Between fyofyofyo@hotmail.com and "ibo ibo"). The Western Union records corroborate that the sale was consummated.

**G. Further Evidence from Ieremenko's Computer**

In November 2012, the U.S. Secret Service obtained the image of a hard drive belonging to a target in another criminal investigation, Oleksandr Ieremenko. Ieremenko is an Ukranian national who was charged in the District of New Jersey in connection with a separate hacking scheme, wherein a group of Ukranian and Russian hackers worked together to steal news releases from Business Wire, Marketwired, and PR Newswire between February 2010 and August 2015. The hackers then passed the stolen news releases to traders who traded based on the stolen content. *See United States v. Tuchynov, et* al, CR 15-390 MCA (D. N.J.); *see also United States v. Korchevsky, et al.*, CR 15-6076 (E.D.N.Y.).[4] The contents of Ieremenko's hard drive as a whole show that Ieremenko and Nikulin worked together on (1) the stolen news releases, (2) stolen LinkedIn information, and (3) other uncharged hacking activity. In general, the government views Ieremenko and Nikulin as co-conspirators. In 2012 specifically, they were both part of a small cohort of Ukranian and Russian hackers—a criminal clique—whose members consulted with one another and sometimes shared resources. While the government will not attempt to adduce all of this background information at trial, it is important context for two types of evidence recovered from the Ieremenko drive that the government will seek to introduce: Skype chats and certain photos and videos.

The Skype chats are from various dates between June and November 2012. In them, Ieremenko uses the Skype name vaiobro and the alias Sergey Shalyapin. Nikulin uses the Skype name dex.007 and

[4] Ieremenko was also later indicted again in the District of New Jersey for a similar scheme in which he and another individual hacked into the SEC's Electronic Data Gathering, Analysis and Retrieval (EDGAR) system and stole thousands of files, including annual and quarterly earnings reports containing confidential, non-public, financial information. The defendants and others then profited by selling access to the confidential information in these reports and trading on this stolen information prior to its distribution to the investing public. *United States v. Radchenko, et al.*, CR 19-30 MCA (D. N.J.)

the alias Yevgeniy Lomovich. The contents of those conversations demonstrate that Nikulin is dex.007. On November 10, 2012, dex.007 sent a link to Ieremenko that contained the password to chinabig01@gmail.com's Afraid.org account, "Zopaqwe1" and a unique cookie that was part of the Afraid.org subscriber information. Records obtained independently from Afraid.org contain that cookie, and show that the Zopaqwe1 Afraid.org account was searching Afraid.org's systems for vulnerabilities on November 10, 2012. Dex.007 also sent Ieremenko, in October 2012, nonpublic LinkedIn user data, including encrypted and unencrypted passwords. Exhibit G (Translation of Excerpt of Skype Chats).

Ieremenko's hard drive also had a folder on it titled "Moscow 2012." That folder's contents included eight short videos. The metadata and the content of the videos show they were made over the course of two days, March 18 and 19, 2012, in Moscow, Russia, during a meeting of the aforementioned criminal clique. The government seeks to introduce two of the eight videos at trial. In the first, Ieremenko is narrating a drive that he describes as the approach to a "summit of bad motherfuckers" at a Moscow hotel. At the end of the video, Ieremenko's friend, who is driving, calls the driver of a black vehicle that pulls in front of them at the hotel an "angry hacker." Ieremenko's hard drive also contained a photograph showing Nikulin at the wheel of the same black vehicle. Exhibit H (Photo of defendant from O. Ieremenko's computer). In the second video, Ieremenko pans the camera around a conference room. Nikulin is seen, as are coconspirators Nikita Kislitsin and Oleg Tolstikh and others. During the recording, the group is discussing plans for an Internet café business. Exhibit I (CD: Video Clips from Computer of Oleksander Ieremenko).

## II. OFFENSES CHARGED

The Indictment charges the defendant with three counts of computer intrusion, in violation of 18 U.S.C. § 1030(a)(2)(C), for the attacks on LinkedIn, Dropbox, and Formspring; two counts of intentional transmission of information, code, or command causing damage to a protected computer, in violation of 18 U.S.C. § 1030(a)(5)(A), for the attacks on LinkedIn and Formspring; two counts of aggravated identity theft, in violation of 18 U.S.C. § 1028A(a)(1), for the use of LinkedIn and Formspring employee access credentials in connections with the attacks on those companies; one count of trafficking in unauthorized access devices, in violation of 18 U.S.C. § 1029(a)(2), for the trafficking of stolen Formspring credentials; and one count of conspiracy, in violation of 18 U.S.C. § 371, alleging

that the defendant conspired to traffic the stolen Formspring credentials.

## III. ANTICIPATED EVIDENCE

The United States has filed motions in limine addressing specific evidentiary questions that are well-suited to pretrial evaluations. This brief addresses some of the other evidence that the government intends to introduce and issues raised at the pretrial hearing.

### A. Evidence Obtained from Domestic Internet Service Providers

The government intends to offer records, including content and subscriber information, obtained from Google, Dropbox, Microsoft Hotmail, and others. In advance of trial, the government has provided the defense with the relevant certifications under Federal Rules of Evidence 902(11) and/or 902(13) and notified the defense of the government's intent to introduce those records pursuant to the certifications. Defendant has not objected to the government's notice. These records, which were obtained from legally valid search warrants or other process served on the providers, are admissible without further authentication.

Pursuant to Federal Rule of Evidence 902(11) and 902(13), certified domestic records of regularly conducted activities or electronic processes are self-certifying and admissible without the testimony of custodial witnesses under Federal Rule of Evidence 803(6)(A)-(C), if the custodian furnishes a written declaration that the records: (A) were made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters; (B) were kept in the course of a regularly conducted activity; and (C) were made as a regular practice. Here, the records satisfy these requirements. Accordingly, while the government is prepared to provide additional bases for authentication of these materials at trial if necessary, including calling a custodian from the provider, the government believes the 902(11) or 902(13) certification satisfies the issue of authenticity, such that a custodial witness would cause unnecessary delay.

### B. Subscriber Records from Russian National Cable Networks Obtained via MLAT

The United States requested and obtained subscriber records from Russia for some of the IP addresses used in the computer intrusions. The government has provided defendant a sworn declaration that the subscriber records were business records made and kept in the ordinary course of business.

Much like Federal Rule of Evidence 902(11) certifications for domestic business records, 18

U.S.C. § 3505 provides that foreign business records are admissible in criminal proceedings if they are "record[s] kept in the course of regularly conducted business activity" and records are made "at or near the time of the occurrence of the matters set forth, by (or from information transmitted by) a person with knowledge of those matters." 18 USCS § 3505(a)(1)(A); *see United States v. Osorio*, No. 88-5523, 1988 WL 83427, at *1 (4th Cir. July 26, 1988). Section 3505 requires that foreign records can be authenticated through a signed certification. See 18 U.S.C. § 3505(a). The declaration provided pursuant to the Russian response to the United States' request under the Treaty With Russia On Mutual Legal Assistance In Criminal Matters, Treaty Doc. 106-22, 1999 U.S.T. LEXIS 163, satisfies all of the requirements set forth. Accordingly, the subscriber records are admissible without any need for calling a custodian to provide live testimony to authenticate the documents. *See United States v. Strickland*, 935 F.2d 822, 831 (7th Cir. 1991) (admitting records and noting Congressional intent to "streamline" admission of foreign business records by substituting § 3505 certification for "the cumbersome and expensive procedures' of live-witness testimony under Rule 803(6)"); *United States v. Al-Imam*, No. 17-cr-00213 (CRC), 2019 WL 2358365, at *4 (D.D.C. June 4, 2019).

**C. Defendant's Statements.**

The United States will introduce defendant's own statements, including statements made in recorded telephone calls, email messages, and chat transcripts. For example, in one recorded telephone call, defendant talks about "hacking the prison" with his girlfriend. Exhibit J (Translation/excerpt of Defendant's Call 159.924 (Nov. 19, 2018)). Fed. R. Evid. 801(d)(2)(A) provides that a party's own statement is directly admissible against the party. *United States v. Matlock*, 415 U.S. 164, 172 (1974) (A party's "own out-of-court admissions . . . surmount all objections based on the hearsay rule . . . and [are] admissible for whatever inferences the trial judge [can] reasonably draw."). As noted below, the statements of others contained in the e-mail and chat conversations in reply to the defendant may be admitted for the non-hearsay purpose to supply context.

**D. Electronic Evidence Obtained by MLAT**

As described above, the government will offer records obtained from Ieremenko's laptop. The laptop was seized during a search executed by Ukrainian officials pursuant to the Treaty With Ukraine On Mutual Legal Assistance In Criminal Matters, Treaty Doc. 106-16, 1998 U.S.T. LEXIS 203. As part

of discovery, the government has produced records of the search and seizure provided by Ukranian officials in response to the Treaty request and the FBI's forensic report for the computer, as well as copies of the Skype chats, videos, and photos that it intends to introduce. A copy of the forensic image was made available for defense review.

Special Agent Richard LaTulip of the United States Secret Service will testify that he traveled to Ukraine to forensically image Ieremenko's computer, and will authenticate the evidence the United States' intends to introduce as obtained from that image. Other records obtained during the search, including a copy of Ieremenko's passport, will be authenticated by the form signed by the executing Ukrainian investigative officer pursuant to the relevant Treaty provision, Article 15, which provides for admissibility of items seized during the execution of searches performed pursuant to the Treaty.

**1. Defendant's Correspondence**

As with other evidence, the chat transcripts obtained via MLAT from the seized computer, and the correspondence contained in the email content obtained via search warrant are admissible where the requirements of the Federal Rules of Evidence are satisfied. The defendant's email and chat communications are admissible non-hearsay because the information is not offered to prove the truth of the matter asserted or does not meet the definition of hearsay under Fed. R. Evid. 801(c).

Statements introduced for a non-hearsay purpose do not violate the hearsay rule. See, e.g., *Anderson v. United States*, 417 U.S. 211, 219 (1974) ("Out of court statements constitute hearsay only when offered in evidence to prove the truth of the matter asserted."); *United States v. Jaramillo Suarez*, 950 F.2d 1378, 1383 (9th Cir. 1991) (noting that where the probative value of a document "was independent of the truth of its contents, the rule against hearsay was not implicated"; pay-owe sheets introduced for the non-hearsay purpose to show the character of the place not for the truth of the statements). As noted below, the statements of the defendant on emails and chat communications are directly admissible against the defendant under Fed. R. Evid. 801(d)(2)(A). The statements of others used in the e-mails and chat communications are admitted not for the truth of the matter but as non-hearsay to supply context. *See, e.g., United States v. Burt*, 495 F.3d 733, 738-39 (7th Cir.) (in prosecution for sexual exploitation of a minor, distributing child pornography, and possession of child pornography, in Yahoo! chat communication involving the defendant and a third party found on the

defendant's computer, the portion from the third party was admissible as non-hearsay and provided context to the conversation); *United States v. Dupre*, 462 F.3d 131, 136-37 (2d Cir. 2006) (in wire fraud prosecution, emails from investors demanding information about defendant's fraudulent scheme were not hearsay when offered not for truth of the assertion that the scheme was fraudulent, but to provide context for the defendant's message sent in response and to rebut defendant's argument that she did not know scheme was fraudulent; no Confrontation Clause issues arose since the statements were offered for a non-hearsay purpose); *United States v. Safavian*, 435 F.Supp.2d 36, 44 (D.D.C. 2006) (admitting some emails which "provide context for the defendant's statements and are not introduced for their truth").

The United States will also introduce automated account messages sent to defendant from victims such as LinkedIn and Dropbox for the non-hearsay purpose of demonstrating that the defendant opened accounts with those businesses in association with his intrusions as part of his method of operating. These automated messages are not hearsay. Courts have consistently held that machine-generated information is not hearsay as no "person" is making a statement. *See, e.g., United States v. Hamilton*, 413 F.3d 1138, 1142 43 (10th Cir. 2005) (computer generated "header" information (including the screen name, subject of the posting, the date the images were posted, and the individual's IP address) was not hearsay; no "person" acting as a declarant). Moreover, these communications show the relationship of the defendant with the victims and the fact of him receiving communications from those companies on relevant dates, and are not offered for the truth of the matters asserted in those communications. *See, e.g., United States v. Siddiqui*, 235 F.3d 1318, 1322 (11th Cir. 2000) ("Those [e-mails] sent by Siddiqui constitute admissions of a party pursuant to Fed. R. Evid. 801(d)(2)(A), and those between Siddiqui and Yamada unrelated to the NSF investigation are non hearsay admitted to show Siddiqui's and Yamada's relationship and custom of communicating by e mail.").

**2. Photos and Videos**

After Special Agent LaTulip has authenticated the image of Ieremenko's hard drive, Special Agent Miller will describe how he reviewed the image. Special Agent Miller is able to recognize at least one person in each video and photograph that the government will seek to admit. FBI Special Agent Emily Odom is able to identify Kislitsin in the second video because she personally interviewed Kislitsin in 2014. The combined testimony of the agents regarding the photos and videos is sufficient

authentication under Fed. R. Evid. 901. *See United States v. Estrada-Eliverio*, 583.F.3d 669, 672 (9th Cir. 2009) ("A party need only make a prima facie showing of authenticity so that a reasonable juror could find in favor of authenticity or identification.") (internal citations omitted). In other words, the exhibits are what they purport to be: videos and photos saved on Ieremenko's computer. *See United States v. Hock Chee Koo*, 770 F.Supp.2d 1115, 1122 (D. Or. 2011) ("The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness. The mere possibility that the logs may have been altered goes only to the weight of the evidence not its admissibility.") *quoting United States v. Bonallo*, 858 F.2d 1427, 1436 (9th Cir. 1998).

As for the statements that are audible in the videos, the statements in the first video are admissible as present sense impressions. The person making the video says at the outset, "In short, we are reporting on the spot. Now, here at this Vega Izmailovo Hotel, there will be a fucking summit of bad motherfuckers." Later, the driver says in reference to the movement of the black sedan, "Look, what an angry person. Angry hacker." The present sense impression exception to the rule against hearsay applies to statements "describing or explaining an event or condition, made while or immediately after the declarant perceived it." Fed. R. Evid. 803(1). One of the key components of this exception is contemporaneousness, which is present. The statements in the video are being made without much reflection. Additionally, many of the statements are readily verified by the footage itself. As the speaker talks about the summit, a large hotel comes into view. Later, the camera pans to an older woman standing outside and the speaker says, "There's a granny over there. Picking her fucking nose." Indeed, the woman visibly removes something from her nose. The statements in the first videos should be admitted pursuant to Rule 803(1). *See, e.g. United States v. Shaw*, 2018 WL 9649495 (C.D. Cal. 2018) (admitting statements in 911 call as present sense impressions).

As for the audio in the second video, that conversation is not hearsay because the United States is not offering it to prove the truth of the matter asserted. The probative value of the video is that it puts three of the alleged co-conspirators in the same room approximately two months before the Formspring hack. Admission of Exhibit 74 is proper under Fed. R. Evid. 401.

**E. Translated Documents and Transcripts**

Among other evidence, the government intends to offer (1) foreign language correspondence that

has been translated into English and (2) audio and video recordings containing Russian that have been transcribed and translated into English. The government intends to offer as substantive evidence all English translations of foreign language documents, recordings, or videos (or any part thereof). This is necessary to allow the jury to properly evaluate foreign-language evidence.

In advance of trial, the government has provided the translations to the defendant. To date, the defense has not disputed the accuracy of any of these transcriptions or proposed revisions or alternative translations. The English transcripts of foreign language correspondence and conversations are admissible as substantive evidence. *See, e.g., United States v. Franco*, 136 F.3d 622, 626 (9th Cir. 1998) (recognizing procedure of admitting both foreign language evidence and translations).

**F. Victim Intrusion Logs**

Some of the evidence at trial will include machine-generated information contained in logs, including those obtained from computers operated by LinkedIn, Dropbox, Formspring, and Automattic[5]. For example, the information in the logs might the IP address of the outside computer connecting to the company, the date and time, account name, user agent string, and cookie. Courts have consistently held that machine-generated information is not hearsay as no "person" is making a statement. *See, e.g., Hamilton*, 413 F.3d at 1142 43 (computer generated "header" information not hearsay); *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir.) (information automatically generated by fax machine is not hearsay since "nothing 'said' by a machine . . . is hearsay"); *United States v. Welton*, No. CR 09-00153-MMM, 2009 WL 10680850, at *3 (C.D. Cal. July 17, 2009) ("The header and footer information in question is generated by a computer independent of human observations or reporting, and thus does not

///

[5] Pending the Court's decision regarding the Automattic evidence.

contain assertions that amount to hearsay.") Because the original records are voluminous, the United States will introduce these records in summary format that can be read and understood by the jury.

DATED: March 3, 2020

Respectfully submitted,

DAVID L. ANDERSON
United States Attorney

/s/
MICHELLE J. KANE
KATHERINE L. WAWRZYNIAK
Assistant United States Attorneys

# Exhibit A

**Excerpt of Summary of LinkedIN VPN Logs for User NBerry**

| ID | User | State | Location | External IP | Internal IP | Status | Date/Time |
|---|---|---|---|---|---|---|---|
| 42278 | nberry | started | United States | 50.78.107.210 | 172.18.36.30 | | 2/29/2012 14:13 |
| 257190 | nberry | disconnected | United States | 50.78.107.210 | | Peer Reconnected | 2/29/2012 17:31 |
| 42658 | nberry | started | United States | 50.78.107.210 | 172.18.36.30 | | 2/29/2012 17:32 |
| 257255 | nberry | disconnected | United States | 50.78.107.210 | | Lost Service | 2/29/2012 18:08 |
| 43152 | nberry | started | United States | 50.78.107.210 | 172.18.36.179 | | 3/1/2012 0:06 |
| 257919 | nberry | disconnected | United States | 50.78.107.210 | | Lost Service | 3/1/2012 0:57 |
| 44133 | nberry | started | United States | 50.78.107.210 | 172.18.36.43 | | 3/1/2012 10:53 |
| 258935 | nberry | disconnected | United States | 50.78.107.210 | | Lost Service | 3/1/2012 12:30 |
| 44573 | nberry | started | United States | 50.78.107.210 | 172.18.36.201 | | 3/1/2012 13:24 |
| 259189 | nberry | disconnected | United States | 50.78.107.210 | | Lost Service | 3/1/2012 14:11 |
| 45652 | nberry | started | United States | 50.78.107.210 | 172.18.36.49 | | 3/2/2012 0:33 |
| 260396 | nberry | disconnected | United States | 50.78.107.210 | | Lost Service | 3/2/2012 1:22 |
| 46437 | nberry | started | United States | 50.78.107.210 | 172.18.36.79 | | 3/2/2012 12:04 |
| 261412 | nberry | disconnected | United States | 50.78.107.210 | | Lost Service | 3/2/2012 15:56 |
| 46956 | nberry | started | United States | 50.78.107.210 | 172.18.36.70 | | 3/3/2012 0:29 |
| 261706 | nberry | disconnected | United States | 50.78.107.210 | | Lost Service | 3/3/2012 1:02 |
| 47315 | nberry | started | Russian Federation | 178.140.107.170 | 172.18.36.204 | | 3/3/2012 7:49 |
| 262079 | nberry | disconnected | Russian Federation | 178.140.107.170 | | User Requested | 3/3/2012 8:28 |
| 47345 | nberry | started | Russian Federation | 178.140.107.170 | 172.18.36.206 | | 3/3/2012 8:29 |
| 262094 | nberry | disconnected | Russian Federation | 178.140.107.170 | | User Requested | 3/3/2012 8:49 |
| 47375 | nberry | started | Russian Federation | 178.140.105.239 | 172.18.36.79 | | 3/3/2012 9:15 |
| 47504 | nberry | started | United States | 50.78.107.210 | 172.18.36.76 | | 3/3/2012 12:55 |
| 262251 | nberry | disconnected | United States | 50.78.107.210 | | Lost Service | 3/3/2012 13:32 |
| 48417 | nberry | started | United States | 50.78.107.210 | 172.18.36.94 | | 3/4/2012 8:33 |
| 263116 | nberry | disconnected | United States | 50.78.107.210 | | User Requested | 3/4/2012 9:26 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 48531 | nberry | started | United States | 50.78.107.210 | 172.18.36.105 | | 3/4/2012 10:00 |
| 48532 | nberry | started | United States | 50.78.107.210 | 172.18.36.105 | | 3/4/2012 10:00 |
| 263145 | nberry | disconnected | United States | 50.78.107.210 | | User Requested | 3/4/2012 10:00 |
| 48533 | nberry | started | United States | 50.78.107.210 | 172.18.36.105 | | 3/4/2012 10:00 |
| 263216 | nberry | disconnected | United States | 50.78.107.210 | | Lost Service | 3/4/2012 10:52 |
| 48740 | nberry | started | United States | 50.78.107.210 | 172.18.36.110 | | 3/4/2012 11:58 |
| 263324 | nberry | disconnected | United States | 50.78.107.210 | | Lost Service | 3/4/2012 12:09 |
| 49114 | nberry | started | United States | 50.78.107.210 | 172.18.36.129 | | 3/4/2012 14:33 |
| 263766 | nberry | disconnected | United States | 50.78.107.210 | | Lost Service | 3/4/2012 15:49 |
| 49263 | nberry | started | United States | 50.78.107.210 | 172.18.36.129 | | 3/4/2012 15:57 |
| 263870 | nberry | disconnected | United States | 50.78.107.210 | | Lost Service | 3/4/2012 16:36 |
| 51547 | nberry | started | United States | 50.78.107.210 | 172.18.36.125 | | 3/5/2012 14:39 |
| 266302 | nberry | disconnected | Russian Federation | 178.140.105.239 | | User Requested | 3/5/2012 16:34 |
| 266366 | nberry | disconnected | United States | 50.78.107.210 | | Lost Service | 3/5/2012 17:05 |
| 52353 | nberry | started | United States | 50.78.107.210 | 172.18.36.98 | | 3/5/2012 23:47 |
| 267193 | nberry | disconnected | United States | 50.78.107.210 | | Lost Service | 3/6/2012 1:08 |
| 53378 | nberry | started | United States | 50.78.107.210 | 172.18.36.134 | | 3/6/2012 10:59 |
| 268870 | nberry | disconnected | United States | 50.78.107.210 | | Lost Service | 3/6/2012 17:11 |
| 54734 | nberry | started | United States | 50.78.107.210 | 172.18.36.138 | | 3/6/2012 23:01 |

# Exhibit B

**Subject:** Jammiro, welcome to LinkedIn!
**From:** LinkedIn <welcome@linkedin.com>
**Date:** 8/3/12 3:03 PM
**To:** Jammiro Quatro <chinabig01@gmail.com>

## Welcome to LinkedIn!

LinkedIn

Make sure recruiters and colleagues see all you have to offer.

Jammiro Quatro

Job Title

Russian Federation | Accounting

Add Photo

| | |
|---|---|
| Current | • Add Company » |
| Past | • Add Past Position » |
| Education | • Add Education » |

Finish Your Profile

**Subject:** Get 16 GB of Dropbox space for free!
**From:** Dropbox <no-reply@dropboxmail.com>
**Date:** 4/10/12 1:46 PM
**To:** chinabig01@gmail.com

# Dropbox

Hi Jammis,

You can now earn **twice as much** free space by inviting your friends!

For each friend that installs Dropbox, you'll both get 500 MB of free space. You can earn up to 16 GB.

Invite your friends now!

Thanks for spreading the Dropbox love,
– The Dropbox Team

P.S. Already invited a bunch of people? Don't worry! You'll get credited for all of them.

**Subject:** Welcome to Formspring
**From:** Formspring <noreply@formspring.me>
**Date:** 6/13/12 9:31 PM
**To:** chinabig01@gmail.com

formspring

**Hi!**

Your account has been created. We hope you have a fun time interacting with friends on Formspring.

**Here are three ways to get the most out of your account:**

Find Friends
Find your friends on Formspring to ask them questions and follow their answers.

Update Your Profile
Personalize your public profile with a photo and other information to help friends recognize you.

Answer Questions
Start answering some questions to start building out your Formspring page.

If you have any questions, please visit our help center.

Thanks,
The Formspring Team

**Formspring is mobile!** Download the official Formspring app for Android or iPhone.





YN001722

# Exhibit C

*Vasiliev*
NKS
NATIONAL CABLE NETWORKS

Recipient's No. *2-10-1632* dated January 30, 20[illegible]
In response to sender's No. 96/11/23 dated January 10, 2013

Attention: Deputy Head of the Bureau of Special Technical Projects of the Main Directorate of the Ministry of Internal Affairs for the city of Moscow

Mr. Ryabov A.A.
127006, Moscow, ul. Petrovka 38

In response to your request dated January 10, 2013 No. 96/11/23 I hereby advise as follows:

Connection (on the date and at the time indicated in the request from the dynamic **IP address 178.140.105.239**) was established from the workstation of the network user of OAO National Cable Networks [Russian abbreviated name OAO NKS]

| | |
|---|---|
| FULL NAME | Nikulin Evgeny Alexandrovich |
| ADDRESS | Moscow, rayion Tsaritsyno, Kantemirovskaya ulitsa, d. 17 kop. 1, p. 6, et. 5, kv. 250 |
| PHONE | (909) 690-90-25 |
| PASSPORT | 45 09 486514 |
| Additional Information | MAC 0025643a6f57<br>Contract No. 5645935, personal account 3121515 |

Connection (on the date and at the time indicated in the request from the dynamic **IP address 178.140.107.170**) was established from the workstation of the network user of OAO National Cable Networks [Russian abbreviated name OAO NKS]

| | |
|---|---|
| FULL NAME | Tonkikh Inga Viktorovna |
| ADDRESS | Moscow, rayion Tsaritsyno, Sevanskaya ulitsa, d. 56, 2, p. 2, et. 5, kv. 88 |
| PHONE | (915) 001-02-10 |
| PASSPORT | 46 08 552274 issued by TP No. 2 in township Lyubertsy |
| Additional Information | MAC 0014d1b956ee<br>Contract No. 6558747, personal account No. 3338818 |

Deputy General Director [signature] S.I. Serov
[ROUND SEAL: Ministry of Internal Affairs of the Russian Federation [illegible]]

Prepared Panchekhin D.A.
Tel.: (495) 795-03-50 Ext. 1106


YN018132

# Exhibit D

**Subject:** Anna Shvedova left a comment to a post on your wall...
**From:** VK
**Date:** 12/21/11, 2:57 PM
**To:** Top Man
**Reply-to:**
"Pavel Durov, inContact.ru Admin"

В КОНТАКТЕ

You have 1 new comment to a post on your wall

**Top Man**

my girl =( is sick
December 21, 2011 at 2:41

**Anna Shvedova**

sick and waiting for her guy..))
December 22, 2011 at 2:57 Reply

Top, you can restrict or disable e-mail notifications in the Notification Settings



YN018046

# Exhibit E

==========
Map Searche
==========

Searched for Staraya Basmannaya, 12 kv. 2
Jun 12, 2011, 6:20:51 PM UTC

Searched for Moscow UL BOLSHAYA NIKITSKAYA D 31
Mar 15, 2011, 2:33:13 PM UTC

Searched for 119019, Central Administrative District, the city of Moscow, ul. Novy Arbat, 15
Apr 21, 2010, 4:55:29 PM UTC

==========
Searches
==========

Searched for linkedin hack
Jun 18, 2012, 7:40:10 AM UTC

Searched for mysql count fields
Jul 27, 2011, 1:47:03 AM UTC

Searched for change mac address wifi windows 7
Jul 26, 2011, 8:44:26 PM UTC

Searched for ul. Ochakovskaya B. d. 11
Jun 6, 2011, 1:24:04 AM UTC

Searched for dkvm-ip1 reset password
May 25, 2011, 3:00:48 PM UTC

Searched for surgemail where users are stored .ini
May 25, 2011, 1:55:16 PM UTC

Searched for pack all files php
May 24, 2011, 11:36:51 PM UTC

Searched for sed remove last 10 symbols
Apr 15, 2011, 3:52:55 PM UTC

Searched for remove unreadable symbols from txt
Apr 15, 2011, 3:50:01 PM UTC

Searched for Podmoskovye Cottage
Apr 15, 2011, 3:20:35 PM UTC

Searched for wordpress vulnerabilities
Apr 15, 2011, 3:20:48 AM UTC

Searched for truecrypt cops hacker
Mar 24, 2011, 3:15:17 PM UTC

Searched for truecrypt hack
Mar 24, 2011, 3:01:35 PM UTC

Searched for installation of ubuntu from the memory drive
Mar 24, 2011, 6:51:06 AM UTC

Searched for installation of ubunty from the network

Mar 24, 2011, 6:49:47 AM UTC

Searched for State Traffic Safety Inspectorate database 2010 online database
Mar 12, 2011, 11:12:04 AM UTC

Searched for change banner to apache
Mar 11, 2011, 7:32:56 PM UTC



YN018113

# Exhibit F

**French-English Translation of Government Exhibits 21A-21D**

*Italic text represents English in original*

…….

From: Dor Fyo
Date: Monday, September 03, 2012 2:48 AM
To: ibo ibo
Subject: Re: hi

*Rais, wait money today*

2012/8/29 ibo ibo <ibob750@gmail.com>
| Monday sorry for the delay Nikita

…….

From: Dor Fyo
Date: Tuesday, August 28, 2012 9:16 AM
To: ibo ibo
Subject: Re: Hi

*So, what about money? Its wednesday already*

*On Friday, August 24, 2012, ibo ibo wrote:*
I give money Monday sorry for the delay Nikita :-(((

…….

…….

From: ibo ibo
Date: Friday, August 24, 2012 2:51 AM
To: Dor Fyo
Subject: Hi

I give money Monday sorry for the delay Nikita :-(((

…….

From: Dor Fyo
Date: Wednesday, August 22, 2012 9:11 PM
To: ibo ibo
Subject: Re: Bonjour

*Ok, wait for money. It's important for me to sell this db soon, because price is very low..*
*Will check sites from your rating. Hope to get money until Friday*

2012/8/21 ibo ibo <ibob750@gmail.com>

> Money before Friday supposedly the client should be returning from abroad
> As for the realsexdates site I'm not interested I gotta have the others
> Did you look back over an email for that did you see it?
>
> Thanks

…….

From: Dor Fyo
Date: Monday, August 20, 2012 9:05 PM
To: ibo ibo
Subject: Re: Hi

*Rais, money today?*
*Also I have this dating site (5.5 Mln users): http://realsexdates.com/*
*Tell me if you are interested*

2012/8/16 ibo ibo <ibob750@gmail.com>

> Tomorrow not possible
>
> Should be Tuesday
>
> For the other sites u got any news?

…….

…….

From: Dor Fyo
Date: Thursday, August 16, 2012 10:07 AM
To: ibo ibo
Subject: Re: Bonjour

*Rais, I'm waiting money, you promised to send it on this week. Tomorrow?*

2012/8/14 ibo ibo <ibob750@gmail.com>

> Look at the top 10 adult sites upper right I need to have one of the 10 sites if possible ]
>
> As for the money it should be this week
>
> Thanks

…….

From: ibo ibo
Date: Thursday, August 16, 2012 12:50 PM
To: Dor Fyo
Subject: Hi

Tomorrow not possible

Should be Tuesday

For the other sites u got any news?

…….

From: ibo ibo
Date: Thursday, August 14, 2012 9:10 AM
To: Dor Fyo
Subject: Bonjour

Look at the top 10 adult sites upper right I need to have one of the 10 sites if possible

As for the money it should be this week

Thanks

…….

…….

From: Dor Fyo
Date: Monday, August 13, 2012 6:55 PM
To: ibo ibo
Subject: Re: Salut

*Probably we can do this site: http://realsexdates.com/*
*Tell me if your client is interested. It may take some time, but seems possible.*

*When do you pay money for that big database?* Wednesday,?

2012/8/13 ibo ibo <ibob750@gmail.com>
> what site is it? name?
>
> As for my client they'd rather have europeen databaes can you do anythijng?
>
> for money it's this week ok?

…….

From: Dor Fyo
Date: Sunday, August 12, 2012 7:26 PM
To: ibo ibo
Subject: Re: Hi

*We can do a porno-site (USA customers) with 5.5 Million users. Are you interested?*

*On Sun, Aug 12, 2012 at 4:28 AM, ibo ibo <ibob750@gmail.com> wrote:*
> ok
>
> On Aug 11, 2012 17:14, Dor Fyo <fyofyofyo@hotmail.com> wrote:
> > *Will try to do such database, I think it's possible.*
> >
> > *Rais, send money to a new name.*
> >
> > ***NAME: OLEG TOLSTIKH***
> > ***CITY: MOSCOW***
> >
> > *Thanks*
> >
> > 2012/8/10 ibo ibo <ibob750@gmail.com>
> > > Ok next week
> > >
> > > Would you have any dbase for adult, porno, x sites??

> I got client for that
>
> On Friday, Aug 10, 2012, Dor Fyo wrote:
> > *Name for money: SERGEY FILIMONOV*
> > *City: MOSCOW*
> >
> > 2012/8/9 Dor Fyo <fyofyofyo@hotmail.com>
> > > *Rais, let's do 5500 Eur. It's really a cheap price for such a big database.*
> > > *When do you plan to send money? Next week?*
> > >
> > > 2012/8/9 ibo ibo <ibob750@gmail.com>
> > > > Nikita i ll offer 5000 Euro for the dbase
> > > >
> > > > All my customers are in vacations annd I only got one offer for now
> > > >
> > > > Maybe he ll pay more but in that case gotta wait to September back from vacation
> > > >
> > > > Tell me what - thanks

…….

From: ibo ibo
Date: Friday, August 03, 2012 1:04 PM
To: Dor Fyo
Subject: Merci

I ll think about it

I ll get back to u soon thanks

…….

From: Dor Fyo
Date: Tuesday, July 31, 2012 11:16 PM
To: ibo ibo
Subject: Re: hi
Attach: [TN: There is a database attached here which includes 1000 e-mail addresses. The file's name is fr1k.csv.]

*Rais, sorry for late answer - i was on the conference in Las Vegas :).*
*Long flights and crazy time, sorry.*
*Example of data is attached*

…….

…….

From: ibo ibo
Date: Monday, July 30, 2012 7:20 AM
To: Dor Fyo
Subject: hi

Where is the sample for the database?

…….
From: ibo ibo
Date: Saturday, July 28, 2012 5:11 AM
To: Dor Fyo
Subject: hi

ok merci

…….

From: Dor Fyo
Date: Friday, July 27, 2012 11:39 AM
To: ibo ibo
Subject: Re: hi

*If you are talking about formspring, right now we have there this info:*

*Email - Nickname - Password hash - IP - Country*

*Address is not in the database, it's a social network - so no address inside, people dont specify it. We can also get real names for users (Nom - Prenom) but this field is optional, so not everybody specified it.*

*I will send you an example of data today\tomorrow*

2012/7/27 ibo ibo <ibob750@gmail.com>

> I want to know if you actually have
>
> Name –First name-address-and email of those member
>
> Can you send me an example?

…….

…….

From: Dor Fyo
Date: Friday, July 27, 2012 10:40 AM
To: ibo ibo
Subject: Re: hi

*You are talking about Formspring database?*

On Friday, July 27, 2012, ibo ibo wrote:

> I want to know if you actually have
>
> Name –Firstname-address-and email of those member
>
> Can you send me an example?

…….

From: Dor Fyo
Date: Thursday, July 26, 2012 9:49 PM
To: ibo ibo
Subject: Re: hi

*What database and what the problem?*

2012/7/26 ibo ibo <ibob750@gmail.com>

> For the *data base* I need
>
> Name firstname emeail address date of birth etc etc
>
> you have what exatly ??

…….

From: Dor Fyo
Date: Thursday, July 26, 2012 9:49 PM
To: ibo ibo
Subject: Re: Hi

*I didn't understand this*

2012/7/26 ibo ibo <ibob750@gmail.com>

> Can you give me more of infos?

…….

…….

From: ibo ibo
Date: Friday, July 27, 2012 2:36 AM
To: Dor Fyo
Subject: hi

I want to know if you actually have

Name –Firstname-address-and email of those member

Can you send me an example?

…….

From: ibo ibo
Date: Thursday, July 26, 2012 4:26 PM
To: Dor Fyo
Subject: Hi

Can you give me more of infos?
…….

From: ibo ibo
Date: Thursday, July 26, 2012 4:08 AM
To: Dor Fyo
Subject: hi

For the *data base* I need

Name firstname emeail address date of birth etc etc

you have what exatly ??

…….

From: ibo ibo
Date: Thursday, July 19, 2012 11:28 AM
To: Dor Fyo
Subject: Hi

Ok i m going to see f its possible
…….

…….
From: Dor Fyo
Date: Wednesday, July 18, 2012 12:00 AM
To: ibo ibo
Subject: Re: hi

*It's fresh database, it wasn't sold to anybody yet. Also I sell db only in one hands.*

*Statistics by countries:*
*USA - 7 Million*
*United Kingdom - 3 Million*
*Europe (Franse Germany Spain etc) - 7 Million*
*Brasil - 5 Million*
*Others - 8 Million*

2012/7/17 ibo ibo <ibob750@gmail.com>

> Thanks for your offer
> But them *data base* were sold how many Times?
> Because for them other that i already bought my customers arent happy they say them Email are over utilized and that people arent reacting
> ur telling me that ur not selling them :-)
>
> On Tuesday, July 17, 2012, Dor Fyo <fyofyofyo@hotmail.com> wrote:
>
> *> Best price in 10.000E, there are 30M users with email, usernames, messages and so on.*
> >
> > 2012/7/17 ibo ibo <ibob750@gmail.com>
> >>
> >> What price pls?
> >> nd i wld like email name firstname etc is that possible ?
> >>
> >> On Tuesday, July 17, 2012, Dor Fyo wrote:
> >>>
> *>>> Rais, I've got a good web-site Formspring.com. It's a very popular and big web-site, it has 30 Million users.*
> *>>> Let me know if you are interested in it*
> >>>
> >>>
> >>> 2012/7/10 ibo ibo <ibob750@gmail.com>
> >>>>
> >>>> Last price for Zappos??
> >>>>
> >>>> U still working or u stopping?For new sites
> >
> >…….

# Exhibit G

# Translation of YN018156: Skype Chat with Evgeny Lomovich

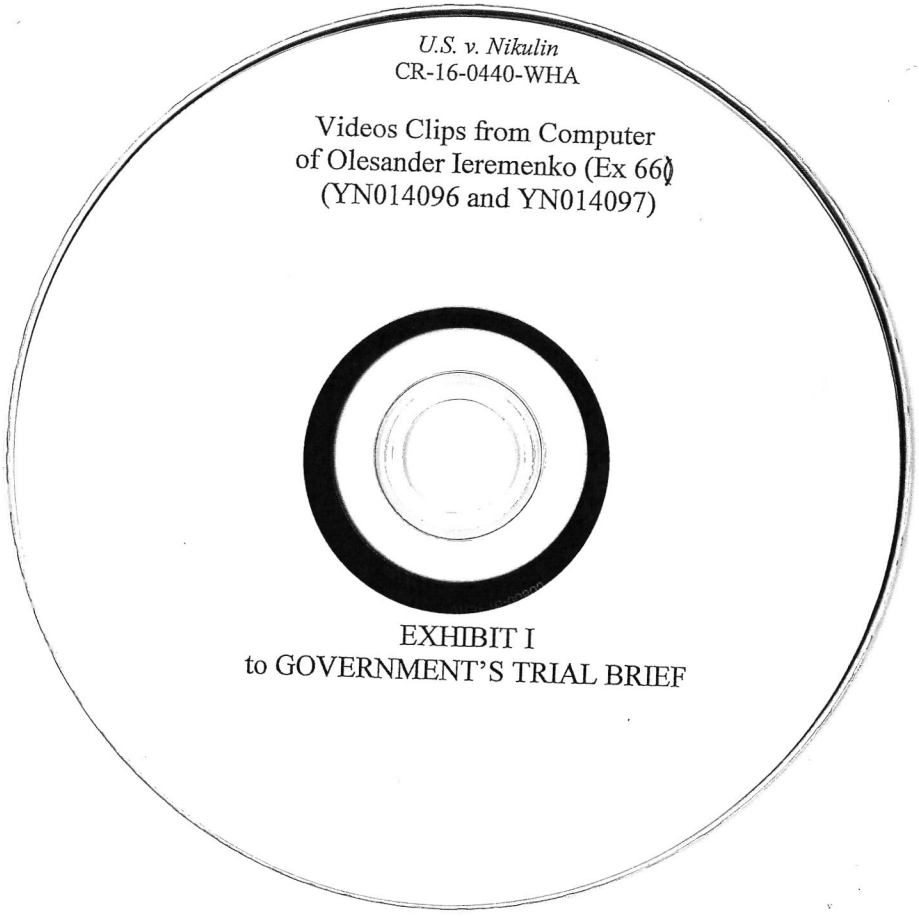
## October 11, 2012

| | | |
|---|---|---|
| Sergey Shalyapin | oo-oo | 11:59 |
| | give me accounts | 11:59 |
| Evgeny Lomovich | send | 14:22 |
| Sergey Shalyapin | kk | 14:22 |
| | 959854,482007,690561,5075793,2933275,43372726,2588336,161425,544837,2168612,2847411,4543430,7261124,1338116,8910915,21397959,25659803,81336861,13655888,47670340,5258959,5258865,27448857 | 15:34 |
| Evgeny Lomovich | 2847411 okambi@gmail.com xxx<br>59854 dhawtof@channelinsight.com 2de690d615d74097f7d0ecd9d481336da3735577<br>2933275 AbelAtl@aol.com 78eec09ec940e522b03501bc54c118cddd9e7ae8<br>161425 jhking@mac.com 015875b16b4764ef297aa69f7c07b8732337cdbb<br>4543430 infrastructureguru@gmail.com xxx<br>482007 kirby56@gmail.com 47834b16c835fdf9eff78274ecc7349f352d29e5<br>544837 James.Piazza@savvis.net f0d61723fdf7301391bea5fff1ef28fa3c7d0eea<br>690561 johnferrandino@gmail.com xxx<br>2168612 marc.capri@savvis.net xxx<br>5075793 dprail@earthlink.net d1f83e08ec9df8e4789f5d7390fd9c61169ac44a<br>5258865 steve.chisholm@gmail.com 0b4a7b4b3033ef472008692111626d1ba050b791<br>5258959 ian.higson@savvis.net 796b9b76324b96b414171230ec22baecae4a8897<br>2588336 jaywantrao@gmail.com 12b6639958f278e5fa04617e940e70e2e352c1be<br>1338116 richard.dresden@savvis.net deaf42bdd33411dc0eaf2ef382478efb28992da6<br>7261124 varghese.thomas@savvis.com 88d70e2f1b3ea253e0beae34f612bb0e79f214b7<br>8910915 christopher.krull@savvis.net 1410b40f4ca7a9fa2a3b10de398a697d5dff4b21<br>13655888 karlwb@gmail.com fb3caac43311b0008a0d22f15851f042c2610353<br>21397959 roger.hill@savvis.net 608d197203b33e6cb9f62e69f28de7a26c451e35<br>25659803 mjpalmer@talktalk.net 3b8b7a62d4ac46538d0e67c465be8bf85af32925<br>27448857 mordimer@gmail.com dbbad92f134f886ac105b12072b96c9982df8c69<br>43372726 amichaelson@sbcglobal.net b566c1c0c7b2892eca7a162688e20a63008dad95<br>47670340 jwsit@hotmail.com xxx<br>81336861 kunalverma.ec@gmail.com xxx | 15:37 |
| Sergey Shalyapin | thks | 15:43 |
| | you confused 59854 and 959854 | 15:45 |
| Evgeny Lomovich | I did it as you gave it to me | 15:45 |
| Sergey Shalyapin | failed to copy the first character =) | 15:45 |
| | failed to include 9 )) | 15:45 |
| | OK, doesn't matter | 15:45 |
| Evgeny Lomovich | 959854 paul@benjes.com 321088bc9df6626e22c54725765e96a49d667fe2 | 15:49 |

# Exhibit H


24
часа

# Exhibit I


*U.S. v. Nikulin*
CR-16-0440-WHA
Videos Clips from Computer
of Olesander Ieremenko (Ex 660)
(YN014096 and YN014097)
EXHIBIT I
to GOVERNMENT'S TRIAL BRIEF

# Exhibit J

**TRANSLATION**

**Date: November 19, 2018**

**Recording: Excerpt of 1542694868_373_13_159_924**

**Male Speaker 1: Yevgeniy Nikulin ("Zhenya")**

**Female Speaker 1: Anya**

**[O/V]: Overlapping Voices**

**[U/A]: Unintelligible audio**

***

Anya: Haven't they told you anything?

Zhenya: I should have got food as well. Neither food nor books and magazines arrived. I asked to bring me computer magazines.

***

Anya: Do you even know what the time is when you call somebody?

Zhenya: I do. The time is okay now. The attorneys work 24/7.

Anya: Zhenya, who said the attorneys work 24/7? If you want everybody to work like that, it doesn't mean everybody wants it.

Zhenya: I hack websites 24/7. I hacked.

Anya: You hack websites?

Zhenya: I hack websites [laughing] You know what? Can you find Artemiy Nevazhno [Артемий Неважно] on ВКонтакте (Russian social network)?

Anya: I know.

Zhenya: Come again?

Anya: I know.

Zhenya: Come again?

Anya: I said I know him. We are friends on ВКонтакте.

Zhenya: You are?

Anya: Yes.

Zhenya: Let him register an American number, I want to call him to talk. Okay?

Anya: Okay.

Zhenya: I want to hack the prison here [laughing].

Anya: Do you want to hack the prison?

Zhenya: I want to hack the prison. The rules here are stupid.

Anya: Okay.

***

Zhenya: Can you ask to send me some magazines. Not just about cars. About computers, about…

Anya: Zhenya, call them in the evening and tell them yourself.

***