No. 17-2479

In the
United States Court of Appeals
For the Second Circuit

UNITED STATES OF AMERICA,

Appellee,

-v.-

FABIO GASPERINI.

Appellant.

On Appeal from a final judgment of conviction entered by the Hon. Nicholas G. Garaufis, Eastern District of New York

APPELLANT'S BRIEF

Simone Bertollini, Esq.
Paul F. O'Reilly, Esq.
Law Offices of Simone Bertollini
450 Seventh Ave, Suite 1408
New York, NY 10123
Tel: (212) 566-3572
simone.bertollini@gmail.com

Counsel for Appellant,
Fabio Gasperini

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES

CASES **Page(s)**

INTRODUCTION

A five-count indictment accused Appellant, Fabio Gasperini of defrauding an Italian advertising company by creating a worldwide botnet which generated "auto-clicks" on internet advertisements.

Following a jury trial, Appellant was found not guilty of all felony counts and guilty of only a single misdemeanor offense under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(2)(C). The trial was held before the Honorable Nicholas G. Garaufis of the Eastern District of New York.

During pre-trial, Appellant moved to dismiss the indictment, arguing, *inter alia*, that the Court had no jurisdiction over "foreign cubed" litigation with no minimum contacts with the United States, and that the "information" allegedly obtained through the alleged scheme was not protected by the overbroad provisions of the CFAA statute. Appellant also moved to suppress emails the government obtained through an extraterritorial application of the Storage Communication Act. The Court denied both motions.

During trial, the District Court allowed the government to introduce unauthenticated copies of hard drives and unauthenticated screenshots from a website known as the "Wayback Machine" over Appellant's objections.

In fact, every defense objection was overruled, and every government objection sustained. Yet, on August 4, 2017, the jury found Appellant not guilty of

all felony charges. The jury found Appellant guilty of one count misdemeanor offense under 18 U.S.C. § 1030(a)(2).

During the sentencing hearing held on August 9, 2017, the government continued to insist—without any factual support—that Appellant had created a worldwide botnet. On this basis, the government sought imposition of the maximum statutory penalties under subsection (a)(2) of the CFAA.

The District Court agreed with the government, despite no witness at trial testifying to having seen a botnet, or that the botnet was ever hosted anywhere. The Court imposed to Appellant an unprecedented sentence of one-year incarceration, a fine of $100,000 and one year supervised release. This appeal followed.

STATEMENT OF APPELLATE JURISDICTION

This Court of Appeals has jurisdiction under 28 U.S.C. § 1291. A notice of appeal was timely filed on August 11, 2017 pursuant to Rule 4(b)(2) of the Federal Rules of Appellate Procedure.

ISSUES FOR REVIEW

1. 18 U.S.C. § 1030(a)(2)(C) punishes *any* unauthorized access to *any* computer that leads to obtainment of *any* kind of information. Does the statute pass muster under the void-for-vagueness doctrine?
2. Is a conviction for a lesser included offense valid when the indictment only contains a factual basis in support of a felony conviction?

3. Is a conviction under 18 U.S.C. § 1030(a)(2)(C) valid without proof of actual access into a protected computer?
4. Is a conviction under 18 U.S.C. § 1030(a)(2)(C) valid without evidence of that access into protected computers was without authorization?
5. Is a conviction under 18 U.S.C. § 1030(a)(2)(C) valid with respect to computers located abroad, when there was no evidence that the use of these computers affected interstate or foreign commerce?
6. Does 18 U.S.C. § 1030(a)(2)(C) protect worthless "information" when no evidence was introduced that the computers' owners tried to market such information?
7. The jury found Appellant guilty of misdemeanor Computer Intrusion after being exposed to evidence related to wire fraud charges that could not have been litigated in a U.S. court. Did Appellant receive a fair trial?
8. Is suppression an appropriate remedy for emails seized abroad through an extraterritorial application of the SCA?
9. Is the admission of unauthenticated screenshots of the "Wayback Machine" in a criminal trial consistent with the Confrontation Clause?
10. Can a lay witness authenticate copies of a hard drives without knowledge of the hard drives content except their "hash" values when there is no evidence showing reliability of the software executing the copy?

11. Can a 19-old misdemeanor conviction be used to impeach an expert witness if no "exceptional circumstance" exist?

12. Can upwards adjustments be applied to a sentence on the basis of facts never proved at trial?

STATEMENT OF THE CASE

This is an appeal against the final judgment of conviction entered by the Eastern District of New York, Hon. Nicholas G. Garaufis, on August 9, 2017.

This appeal also challenged the District Court pretrial rulings, namely:

1. Order on Appellant's first motion to dismiss;[1]
2. Order on Appellant's second motion to dismiss;
3. Order on Appellant's motion to suppress evidence;[2]
4. Order on Appellant's first motion *in limine*;[3]
5. Order on Appellant's fifth motion *in limine*.

[1] *United States v. Gasperini*, No. 16-CR-441 (NGG), 2017 U.S. Dist. LEXIS 84116 (E.D.N.Y. May 31, 2017).

[2] *United States v. Gasperini*, No. 16-CR-441 (NGG), 2017 U.S. Dist. LEXIS 110623 (E.D.N.Y. July 13, 2017).

[3] *United States v. Gasperini*, No. 16-CR-441 (NGG), 2017 U.S. Dist. LEXIS 114166 (E.D.N.Y. July 21, 2017).

SUMMARY OF ARGUMENT

The misdemeanor provision under 18 U.S.C. § 1030(a)(2)(C) is invalid under the void-for-vagueness doctrine, because it punishes *any* unauthorized access to *any* computer that leads to obtainment of *any* sort of information.

Second, the misdemeanor conviction should be reversed because the facts alleged in the indictment and presented at trial by the government could only support a felony conviction under 18 U.S.C. § 1030(a)(2)(C), and Gasperini was not given sufficient notice to defend the lesser included charge.

Third, there was no evidence to convict Appellant. The indictment alleged that Appellant had set up a botnet to further a click fraud scheme, and that he obtained information from protected computers that connected to his botnet. Because there was no evidence that a botnet ever existed, Appellant was acquitted of all fraud-related charges. And no evidence was introduced at trial that Appellant actually accessed any protected computer without authorization.

Fourth, even assuming that actual access into protected computers was proven, the conviction should be reversed as a matter of law because the "information" obtained is of a kind that becomes public every time the device is connected to the internet. And there was no evidence that the QNAP owners were ever deprived of the full use of such information—or tried to market such

information. In short, the conviction was premised on "information" that is not protected by 18 U.S.C. § 1030(a)(2)(C).

Fifth, the misdemeanor conviction was obtained after improperly influencing the jury with evidence in support of a wire fraud case that could not have been litigated in the United States as a matter of law.

Sixth, a large part of the evidence introduced by the government consisted of unauthenticated emails improperly seized through an extraterritorial application of the SCA. The District Court erroneously denied Appellant's motion to suppress.

Seventh, the Court permitted the government to introduce unauthenticated screenshots from the "Wayback Machine," in violation of the Confrontation Clause.

Eight, a substantial part of the evidence against Gasperini consisted of *copies* of hard drives seized in his apartment. The government did not explain why the *original* hard drives were not available. More importantly, the Court improperly allowed a lay witness to authenticate the *copied* hard drives on the sole basis of their "hash" value—without any evidence of the reliability of the software that produced such copies.

Ninth, there were no "exceptional circumstances" present to permit the government to impeach the defense's only witness with a 19-old misdemeanor conviction.

Finally, the sentence imposed on Gasperini was illegal, because it was based on enhancements calculated on charges for which he was acquitted, and that could not have been litigated in the United States in the first place.

ARGUMENT

I. THE CONVICTION SHOULD BE REVERSED BECAUSE 18 U.S.C. § 1030(a)(2)(C) IS FACIALLY UNCONSTITUTIONAL

The void-for-vagueness doctrine is rooted in the Due Process Clause.[4] It includes two distinct and largely independent tests: fair notice, and discriminatory enforcement.[5] The fair notice test asks whether the law is "so vague and standardless that it leaves the public uncertain as to the conduct it prohibits."[6] If a law is so vague that a person cannot tell what is prohibited, "it leaves judges and jurors free to decide, without any legally fixed standards, what is prohibited and what is not in each particular case."[7]

The CFAA is essentially a computer trespass statute. It prohibits trespassing on to a computer much like a trespass statute punishes trespassing onto physical land. The CFAA contains a number of different crimes, but the best way to

[4] *United States v. Williams*, 128 S. Ct. 1830, 1845 (2008).

[5] See *City of Chicago v. Morales*, 527 U.S. 41, 56 (1999).

[6] *Giaccio v. Pennsylvania*, 382 U.S. 399, 402 (1966).

[7] *Id.* at 402–03.

understand the statute is to focus on its broadest section, 18 U.S.C. § 1030(a)(2)(C). This provision punishes whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains [. . .] information from any protected computer."

What does it mean to "access" a computer? The terms "access" and "without authorization" are not defined by the CFAA. Does looking at a coworker's computer screen satisfy the "access" requirement? At least one District Court reached the questionable conclusion that a person can "obtain information," by merely observing it.[8]

Also, the definition of "protected computer" is overbroad and vague.

The definition of "computer" has been held to include "any device that makes use of a electronic data processor."[9] Given that many everyday items include electronic data processors, the definition might plausibly include everything from many children's toys to some of today's toasters and coffeemakers.

In 2008, Congress amended the definition of "protected" computer to include any computer "used in or affecting interstate or foreign commerce or

[8] See, e.g., *United States v. Tolliver*, 2009 WL 2342639 (E.D. Pa. 2009) (citing S. Rep. No. 99-432 at 2484 (1986)).

[9] *United States v. Kramer*, 631 F.3d 900, 902 (8th Cir. 2011).

communication."[10] In federal law, regulation that "affects interstate or foreign commerce" is a term of art: it means that the regulation shall extend as far as the Commerce Clause allows.[11]

It has been held that every computer connected to the internet is a protected computer. Considering that nowadays even TVs and refrigerators are connected to the internet, every electronic device would have to be deemed a "protected computer". However, criminal laws are subject to strict interpretation, and there is no indication that Congress intended for every computer connected to the internet to be a "protected computer".

More importantly, what is the "information" protected by the statute? The few cases prosecuted under section (a)(2) generally deal with the dramatic facts of an employee who accessed a sensitive and valuable database to gather data that could be used to establish a competing company. But how sensitive does the database need to be? How valuable does the data need to be? The statute does not require that the information be valuable or private.

Simply put, 18 U.S.C. § 1030(a)(2)(C) punishes:

> *any* unauthorized access,

[10] 18 U.S.C. § 1030(e)(2)(B).

[11] See *Russell v. United States*, 471 U.S. 858, 849 (1985).

to *any* protected computer,

that retrieves *any* information,

of *any* kind, interstate or intrastate.

Here, the indictment did not even list *what* information was allegedly obtained by Appellant. The government later served a bill of particulars, listing "information" that becomes public on the internet every time a computer connects to the internet, or items "obtained" by Appellant from how own servers. Because the indictment did not list such "information", it is not realistic to believe that such items were even presented to the Grand Jury.

And as the trial proceeded, the government continued to fill the "information" list with items not even listed in the bill of particulars. For instance, the prosecutor told the jury that the QNAP "architecture type" is valuable "information" because it was useful to tailor the "shellshock" attack.

In sum, 18 U.S.C. § 1030(a)(2) is overbroad and does not pass the void-for-vagueness

II. THE CONVICTION SHOULD BE REVERSED BECAUSE THE INDICTMENT DID NOT PROVIDE SUFFICIENT NOTICE OF THE LESSER INCLUDED OFFENSE

The indictment charged Appellant with setting up and operating a worldwide botnet to further "click fraud" scheme.

Count Two of the indictment reads:

> On or about and between February 2011 and June 2016, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant FABIO GASPERINI, together with others, did knowingly and intentionally access, and attempt to access, one or more computers without authorization and exceed authorized access, and thereby did obtain information from one or more protected computers for the purpose of commercial advantage and private financial gain, and in furtherance of criminal and tortious acts in violation of the laws of the United States and any State, and the value of the information obtained exceeded $5,000.
> APP-31.

The indictment consistently—and unequivocally—alleged that Appellant intruded into computers and set up a botnet to further a "click fraud" scheme.

> It was a part of the scheme that the defendant FABIO GASPERINI, together with others, accessed the compromised servers without permission and installed on them malicious software that gave him remote access to, and control of, these compromised servers, which together constituted a botnet. In establishing this botnet, GASPERINI also obtained unauthorized access to sensitive data and files stored on the compromised servers.
> A-30.

The government had also charged Appellant with violating subsection (a)(4) of the CFAA. The indictment reads:

> [. . .] FABIO GASPERINI, together with others, did knowingly and with intent to defraud access, and attempt

> to access, one or more protected computers without authorization, and exceed authorized access, and by means of such conduct did further the intended fraud and obtain something of value, to wit: the use of a computer, information, and United States and foreign currency.

The jury acquitted Appellant of all the felony counts of the indictment, and convicted him of the misdemeanor offense under 18 U.S.C. § 1030(a)(2).

This means that the jury concluded that the computer intrusion:

> was *not* committed for purposes of commercial advantage or private financial gain;
>
> was *not* committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; and that
>
> the value of the information obtained did *not* exceeded $5,000.

More importantly, the computer intrusion was not committed with intent to defraud. Otherwise, the jury would have convicted Appellant under (a)(4), which requires that the "information" be just "valuable", without setting forth any minimum threshold.

In sum, in convicting Appellant under the misdemeanor provision of (a)(2), the Jury could have only concluded that:

> Appellant accessed the QNAP devices without a commercial purpose, without intent to defraud, without furthering any other crime, and the value of the

> information obtained was anything between $0.01 and $4,999.99

The problem is that the indictment accused Appellant of "click fraud", and nowhere in the document was there any mention of any intrusion committed for a non-commercial purpose. Notably, Count Two of the indictment specifies that "the value of the information obtained exceeded $5,000". A-32.

The question is whether the indictment gave Appellant sufficient notice that he was being prosecuted for a computer intrusion committed for a non-fraudulent or non-commercial purpose.

Perhaps the principle most basic to the notion of due process is the requirement that the defendant have notice of the charges made against him, in order that he have an opportunity to defend himself against the charges.

The sixth amendment states "[i]n all criminal prosecutions, the accused shall enjoy the right ... to be informed of the nature and cause of the accusation."[12] Because this right of notice is basic to our adversary system of criminal justice, it is part of the "due process of law" that is guaranteed by the fourteenth amendment to defendants in the criminal courts of the states.[13]

---

[12] See, e.g., *In re Oliver*, 333 U.S. 257, 273 (1948) (right to reasonable notice of charges basic to our system of jurisprudence); *Powell v. Alabama*, 287 U.S. 45, 69 (1932) (notice is an essential element of due process); *Holden v. Hardy*, 169 U.S. 366, 389 (1897) (same).

[13] *Faretta v. California*, 422 U.S. 806 (1975).

While it is possible to read an indictment on one charge as notice that, in addition, some lesser included offense may also be charged, due process requires that the defendant have notice of which offense that is.[14]

Here, there is no plausible reading of the indictment that would even remotely suggest that Appellant was being prosecuted for a computer intrusion committed for ludic, educational, or any other non-fraudulent, non-commercial or non-felonious purpose.

Instead, the indictment reiterated multiple times that the computer intrusion was designed to commit "click fraud," which was described as a scheme to defraud advertising companies to achieve a monetary gain. Even during trial, the government asked their expert to assign a value to the hypothetical botnet.

In sum, the language of the indictment and the theory presented at trial by the government were clear and unequivocal: the computer intrusion was committed to defraud and/or make a profit.

Under these circumstances, it is clear that Appellant did not have sufficient notice before trial that he was charged with the lesser included offense under Count Two of the indictment.

[14] See, e.g., *Russell v. United States*, 369 U.S. 749, 768 (1961) (indictment must set out specific offense with which defendant charged); *United States v. Milk Distributors Ass'n*, 200 F. Supp. 792, 802 (D. Md. 1961) (same).

III. THE CONVICTION SHOULD BE REVERSED BECAUSE GASPERINI DID NOT UNLAWFULLY ACCESS ANY PROTECTED COMPUTER

Appellant was found guilty of a misdemeanor count under 18 U.S.C. § 1030(a)(2)(C), which is essentially a simple computer trespass statute that does not require intent to defraud or a commercial or private financial gain.

At trial, the government's lay and expert witnesses were unable to say whether or when Appellant had ever accessed a QNAP device in the United States. Moreover, while another government's expert witness testified that a hard drive seized in Appellant's apartment contained evidence of login session into four QNAP devices located *abroad*, there was *no* evidence to establish that such accesses were "unauthorized."

A. There was no evidence of access into any U.S-based QNAP device.

During trial, Dr. Johannes Ullrich—the government's most prominent expert witness—testified that the malicious script he examined would intrude into a vulnerable, or, "unpatched" QNAP device and create a "backdoor" through SSH service port 26.

Dr. Ullrich also testified that if an infected QNAP device did not have SSH port open, it would "probably not be infected" with the same version of the malicious script.

> Q So if you have a QNAP device that doesn't have that part[15] open, would that QNAP be infected or not infected by this particular virus?
>
> A It will probably not be infected.
>
> See A-107 ¶ 17.

Mr. Luis Cruz, another government witness, testified that the QNAP he analyzed did not have port 26 open.

> Q Okay. So, what's the status of port 26 on your nmap analysis?
>
> A Port 26, it's not shown.
>
> Q Does that mean it's closed?
>
> A Yes, it means it's closed.
>
> See A-126 ¶¶ 2-6.

In other words, at trial, there was no evidence that the three QNAP devices located in New York were even affected with the same malware that the government alleged was being spread by Appellant!

Even if there was sufficient evidence that the script was the same, none of the QNAP owners located in the U.S. testified at trial that Appellant ever accessed their device, much less that he obtained, extracted, or even viewed any information therein contained.

[15] It should be "port"

Once infecting the QNAP device, the alleged computer program created a new user and password, or "backdoor." Without any evidence of actual access, however, this would be analogous to creating a key someone's house without ever using it to open the door.

Actual access to the QNAP devices was not even *alleged* in the indictment. Without a shred of evidence of actual access into a protected computer, Appellant could not be convicted of computer intrusion for copying access credentials but never actually using them.

The CFAA simply does not punish this kind of conduct. Even giving the maximum possible weight to the evidence presented by the government at trial, no conviction under 18 U.S.C. § 1030(a)(2) could be sustained because the conduct alleged by the indictment does not fit the statute. The extensive interpretation of the CFAA proposed by the government would certainly obviate the absence of a "click fraud" statute, except that criminal statutes are subject to strict construction.

i) There was no evidence that information was obtained.

The government has nonetheless argued that information was obtained when the compromised QNAP devices connected to the imaginary botnet the government claims Appellant was in control of.

The following is an excerpt of the cross examination of Dr. Ullrich:

> Q The question is isn't it true that with respect to this bot net, you declare that: It is not a full-fledged command

> and control server in that it doesn't appear to send any commands, nor does it track the system, look for updates, from the bot. Right now, I don't think that is happening. Is that accurate?
>
> A It's probably accurate. That's what I said at the time. I don't remember the exact statement.
>
> Q If this article came out on December 15 and in this article you're saying that these bots, these infected QNAP devices don't go anywhere, can these infected QNAP make any click through the botnet?
>
> A This was a day or so after, yes, at that time it's very likely that the command control server was shut down.
>
> Q So, by December 15, if there's no control banner[16], there's no click from the traffic device, correct?
>
> A Correct.
>
> See A-104 ¶¶ 3-19.

The question is whether a botnet's control panel had ever existed. There is simply not a shred of evidence of that, let alone evidence beyond a reasonable doubt. The District Court allowed the government to introduce unauthenticated pictures of an IRC chat as "evidence" of a control panel. Even with such a questionable evidentiary ruling, an impartial jury could not find sufficient evidence that a botnet ever existed.

[16] It should be "control panel".

Mr. Luis Cruz, another government expert, also testified that he never saw the botnet:

> Q Have you ever seen this particular botnet operated?
>
> A Out in the wild, no.
>
> Q Say that again, sorry.
>
> A Out in the Internet, no.
>
> Q So, you only saw it on paper.
>
> A Yes.
>
> See A-124 ¶¶ 16-21.

After all, if the jury believed that Appellant had set up and operated a botnet to generate "auto-clicks," they would have convicted him of one of the felony count under 18 U.S.C. § 1030(a)(2)(C), which requires an intent to accomplish a private gain of *any* amount.

If there was no evidence of a botnet, and no proof of actual access into the devices, how exactly did Appellant "obtain information?"

B. There was no evidence that access to the four QNAP devices located abroad was unauthorized.

During trial, a government expert testified that one of the hard drives seized at Appellant's apartment contained browsing sessions to four I.P. addresses

corresponding to QNAP devices along with references to the access credentials created by the script.

First, there was no evidence that the credentials actually worked on these four devices. Second, even assuming that the evidence was sufficient to prove access, there was not a shred of evidence that such accesses were unauthorized. The four QNAP devices could have belonged to anyone, such as individuals that gave Appellant permission to test the vulnerability of their systems, or they could just be Appellant's devices. Finally, even if there was evidence to prove actual, unauthorized access, Appellant could not be convicted of intruding into QNAP devices located abroad, because there was no evidence whatsoever that any of these QNAP's qualified as a "protected computer."

During cross examination, Mr. Cruz testified:

> Q Do you know the owner of any of these four QNAP devices?
>
> A No, not the owners, no.
>
> Q Have you ever examined any of these four QNAP devices?
>
> A "Examined" as in?
>
> Q The physical device.
>
> A Physical device or forensic image? No.

> Q Have you tried to log into any of these device?
>
> A No.
>
> Q So, you didn't input the user name "request."
>
> A Negative, no.
>
> Q So you don't know if that would actually had worked, correct?
>
> A Correct.
> See A-127, 128 ¶¶ 23-25, 1-10.

Mr. Cruz also testified that these four QNAP devices were not based in the United States.

> Q Are you aware that none of those 12 IP addresses that you found as a reference in the hard drive are not American?
>
> A I don't understand the last part of your question.
>
> Q Are you aware that none of the 12 IP addresses are U.S. based?
>
> A Yes, I am aware. I did look up the three or four that I was able to connect to and they were assigned to Italy and Australia.
> See A-129 ¶¶ 16-23.

The government did not introduce any evidence that these four QNAP devices located abroad were used or affected U.S. interstate commerce.

IV. THE CONVICTION SHOULD BE REVERSED BECAUSE THE INFORMATION OBTAINED IS NOT PROTECTED BY THE CFAA

According to the Bill of Particulars, the "information" allegedly obtained consisted of intangible, non-proprietary, worthless personal identifiers, browser information, and server configuration command lines. See APP 38-40.

Moreover, the government included items that were allegedly planted by Appellant himself into infected computers—as opposed to being "obtained"—such as the malware, user information, passwords. Finally, the government included items that were found in the servers allegedly leased—and paid for—by Appellant—rather than inside infected computers.

In other words, Appellant did not take any "information" within the meaning of the CFAA.

The reason is straightforward: the auto-click scheme described by the indictment does not need to take *any* information in order to function—all that is needed is a computer and bandwidth to click on banner ads.

The Third Circuit has already reached the issue on whether obtainment of "personal identifiers" listed in the Bill of Particulars such as a computer's IP address, and a user-agent string, supports a cause of action under 18 U.S.C. § 1030.[17]

[17] See *In re Google Inc.*, 806 F.3d 125, 130 (3d Cir. 2015).

In the *Google* case, the defendant implanted software, commonly known as tracking "cookies" on the plaintiffs' personal computers.

The Court opined:

> In view of our common sense reading of the operative allegations of the complaint, we note the factual position that the defendants advanced at argument:
>
> "*The cookie doesn't acquire anything. . . The cookie doesn't look for anything. It just sits on the browser and gets sent along with information that would otherwise be sent*."
>
> The information at issue would be sent anyway because "the user's web browser send[s] a GET request to Google to display the relevant advertising information for the space on the page for which Google has agreed to sell display advertisements."[18]
> *Id.* at 142. (emphasis added)

The Third Circuit agreed with Google's position that tracking cookies do not acquire or search for anything within the "infected" computer and held that such cookies did not violate the CFAA. The Court reasoned that any computer connected to the internet would be sending the same "information" every time a browsing request was entered by the user.

Here, any "protected computer," which has been held to be any computer

[18] *Id.* at 142.

any computer connected to the internet, has already made available to the internet its IP address, user-agent string, etc., in order to be connected to the internet and visit websites. This is neither information nor anything of value.

The alleged intrusion here was even slighter than the intrusion described in the *Google*, as there were no allegations that Appellant's software monitored and tracked every website the users visited. By contrast, tracking cookies, which are routinely placed on computers, track and record of every single webpage the user clicks on.

Is there any difference with the script allegedly planted by Appellant into various computers? The answer is no.

When dismissing the 18 U.S.C. 1030 cause of action, the Third Circuit opined that:

> "The complaint plausibly alleges a market for internet history information such as that compiled by the defendants. Further, the *defendants' alleged practices make sense only if that information, tracked and associated, had value*.
>
> However, when it comes to showing "loss," the plaintiffs' argument lacks traction. They allege no facts suggesting that they ever participated or intended to participate in the market they identify, or that the defendants prevented them from capturing the full value of their internet usage information for themselves.

> For example, they do not allege that they sought to monetize information about their internet usage, nor that they ever stored their information with a future sale in mind.
>
> Moreover, the plaintiffs do not allege that they incurred costs, lost opportunities to sell, or lost the value of their data as a result of their data having been collected by others". (emphasis added)[19]

In citing the *Google* decision, the Southern District of New York opined that the value of a user's browser information was too conjectural:

> While we recognize that browsing information may possess value in the abstract, absent allegations suggesting that plaintiffs' ability to monetize their browsing information was diminished, this alleged harm remains too conjectural.
>
> The Third Circuit in Google persuasively rejected similar allegations in analyzing whether the plaintiffs had pled statutory "loss" under the CFAA [. . .][20]

The Southern District also noted that this case was different from those involving a cognizable injury to its "property right" in keeping confidential and

[19] *Id*. at 148-149.

[20] *Mount v. PulsePoint, Inc.*, 2016 U.S. Dist. LEXIS 112315 at 18 (S.D.N.Y. Aug. 17, 2016).

making exclusive use of information concerning its business plans when others exploited the information for insider trading purposes.[21]

In an unreported decision, this Court of Appeals later affirmed the judgment of the District Court, holding that "[P]laintiffs do not allege that PulsePoint's data collection practices actually deprived them of any opportunity to sell their own personalized information."[22]

The Government combined the words "United States and foreign currency" and "use of a computer" within the same category of "something of value" in an attempt to elude the requirement of alleging the computer use value and confuse the Grand Jury.

V. THE CONVICTION SHOULD BE REVERSED BECAUSE ALL THE EVIDENCE RELATED TO AN ITALIAN MATTER BEING LITIGATED IN A U.S. COURT

Appellant was convicted of a single count of misdemeanor Computer Intrusion for obtaining information. The verdict is the product of the undue influence of the massive amount of evidence introduced at trial in support of the Wire Fraud and Money Laundering counts of the indictment.

[21] *Id.* at 19-20.

[22] *Mount v. PulsePoint, Inc.*, 684 F. App'x 32, 36 (2d Cir. 2017).

As explained above, the government charged Appellant of engaging in "click fraud." However, the only alleged victim of the click fraud scheme was LeonardoAdv, an *Italian* advertising company based in Italy.

There was no legal basis to litigate this case in the Eastern District of New York, much less in any other U.S. Court. United States law governs domestically, but does not rule the world.[23]

The Government alleged that Appellant, an *Italian citizen residing in Rome*, set up and operated a botnet of 140,000 computers across more than 70 countries, to defraud LeonardoADV, an *Italian* company.

There was no allegation and no evidence presented at trial that Appellant obtained U.S. currency, or that JuiceADV wired money to Appellant using a bank located within the United States.

Appellant should not have been prosecuted in the United States, because the Wire Fraud statute does not apply extraterritorially.

In *Morrison v. Nat'l Australia Bank Ltd.*, the Supreme Court considered the extraterritorial application of Section 10(b) of the Securities Exchange Act.[24] The

[23] See *Kiobel v. Royal Dutch Petro. Co.*, 133 S. Ct. 1659, 1664 (2013).

[24] *Morrison v. Nat'l Australia Bank Ltd.*, U.S. 247, 254, 130 S. Ct. 2869, 177 L. Ed. 2d 535 (2010).

Court held without dissent that "[w]hen a statute gives no clear indication of an extraterritorial application, it has none."[25]

Although Morrison was a civil case, the Court stated that it applies "the presumption [against extraterritorial application] in all cases."[26]

Additionally, the Court held that inferences regarding what Congress might have intended are insufficient; for a court to apply a statute extraterritorially, Congress must give a "clear" and "affirmative indication" that the statute applies extraterritorially.[27]

Here, the Government alleged that, while in Rome, Italy, Appellant committed Wire Fraud by soliciting payments from an *Italian* company based on a "click fraud" scheme carried out using some 140,000 servers across more than 70 countries.

The government offered no proof at trial that any U.S. company was a victim of the alleged scheme. While deliberating, the Jury requested proof of payments from U.S. companies to the "victim" LeonardoADV as they related to Appellant. The Court advised the Jury that there was no such evidence. See ECF

[25] *Id.* at 255.

[26] *Id.* at 261.

[27] *Id.* at 265; see also *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1665, 185 L. Ed. 2d 671 (2013).

169. And as discussed above, the government also offered no testimony or proof that Appellant accessed computers located in the United States.

In *European Community v. RJR Nabisco, Inc.*, 764 F.3d 129 (2d Cir. 2014), this Court of Appeals opined that:

> "[t]he wire fraud and money fraud statutes, as well as the Travel Act, do not overcome Morrison's presumption against extraterritoriality."[28]

In that case, the Court carved out a narrow exception to this rule, concluding that jurisdiction over defendant was proper because the schemes themselves were *directed at the United States* and had a *substantial domestic effects*.[29]

Here, by contrast, the evidence at trial showed that, at best, the alleged scheme was directed towards an *Italian* company. There was *no* evidence at trial that Appellant's scheme was directed at the United States or any U.S. person or U.S. business, let alone that his actions created substantial domestic effects.

In examining the extraterritorial application of RICO, the Supreme Court ruling in *RJR Nabisco* did not alter the principle set forth by the Second Circuit with respect to the Wire Fraud statute. To be clear, Appellant was *not* charged with RICO. But the Government's argument would fail even if that was the case.

[28] *Id.* at 139.

[29] See *Id.* at 142.

The Supreme Court opined:

> "At the first step, we ask whether the presumption against extraterritoriality has been rebutted—that is, whether the statute gives a clear, affirmative indication that it applies extraterritorially. [. . .]
> If the statute is not extraterritorial, then at the second step we determine whether the case involves a domestic application of the statute, and we do this by looking to the statute's "focus."
>
> If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad;
>
> but if the conduct relevant to the focus occurred in a foreign country, then the case involves an impermissible extraterritorial application regardless of any other conduct that occurred in U.S. territory.[30]

Under the Second Circuit's ruling, the Wire Fraud statute does *not* apply extraterritorially. A foreign national acting abroad, with the alleged intent to defraud a foreign company has nothing to do the United States.

In denying Appellant's motion to dismiss, the District Court decided to follow the test set forth in *United States v. All Assets Held at Bank Julius, Baer & Co.*,[31] to determine whether the indictment alleged sufficient domestic conduct.

---

[30] *RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090, 2101 (2016).

[31] *United States v. All Assets Held at Bank Julius, Baer & Co.*, 2017 U.S. Dist. LEXIS 63758.

Under *Bank Julius*, "a complaint alleges a domestic application of wire fraud when (1) a defendant or coconspirator commits a substantial amount of conduct in the United States, (2) the conduct is integral to the commission of the scheme to defraud, and (3) at least some of the conduct involves the use of U.S. wires in furtherance of the scheme to defraud.[32]

Here, the government accused Appellant of hacking into 140,000 computers around the world, roughly 2,400—or 1.7%—of them, allegedly being in the United States, to further a wire fraud directed at an Italian company. Appellant had never entered the United States before being extradited.

Put it differently, the alleged click fraud scheme occurred *exclusively* abroad, and was directed at an Italian company. The alleged use of hacked computers located in the U.S. was a collateral vehicle of the click fraud scheme, rather than the "focus" of the Wire Fraud statute.

A computer intrusion is *not* an element of the Wire Fraud statute. So how can a computer intrusion be the "focus" of the Wire Fraud Statute? If that was the case, the United States would have jurisdiction over crimes committed abroad by individuals using mail services or social networks whose servers—or "wires"—are located within the United States.

[32] Id. at 41.

The District Court simply did not have any authority to conflate the Wire Fraud and Computer Intrusion statutes to help the government prosecute a click fraud statute that does not exist.

The jury convicted Appellant of misdemeanor computer intrusion because they were overwhelmed with all the wire fraud and money laundering allegations. Appellant did not receive a fair trial, and his conviction should be reversed.

VI. THE CONVICTION SHOULD BE REVERSED BECAUSE THE GOVERNMENT INTRODUCED EVIDENCE AT TRIAL THAT WAS ILLEGALLY SEIZED ABROAD

A. The SCA Warrant was impermissibly applied extraterritorially.

This Court of Appeals held that the Stored Communications Act, 18 U.S.C. § 2701 *et. seq*. ("SCA") did not apply "extraterritorially," and therefore the SCA's provisions could not be used to effect a search and seizure of electronic communications stored outside the U.S.[33]

The SCA "was born from congressional recognition that neither existing federal statutes nor the Fourth Amendment protected against potential intrusions on individual privacy arising from illicit access to stored communications in remote computing operations and large data banks that stored e-mails."[34]

---

[33] *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016) rehearing en banc denied No. 14-2985, 2017 WL 362765 (2d Cir. Jan. 24, 2017) (hereinafter "*Microsoft*").

[34] *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 145 (3d Cir. 2015) cert. denied (2016).

Indeed, many of the SCA's provisions prevent third parties from accessing electronic communications without authorization. Section 2703(a)-(c) of the SCA permits the Government to obtain from an email service provider, such as Google, a user's electronic communications provided the Government obtains a warrant that has been issued using the same procedures set forth in Rule 41 of the Federal Rules of Criminal Procedure.

Rule 41 describes the procedures for the issuance of a search and seizure warrant. Of particular relevance here is Rule 41(b)(5) which provides the following:

> (5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within the following:
>
> (A) a United States territory, possession, or commonwealth;
>
> (B) the premises - no matter who owns them - of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or
>
> (C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

As can be seen above, Rule 41(b)(5) generally restricts the geographical reach of a warrant's execution, if not in another federal district, to "a United States territory, possession, or commonwealth," and various diplomatic or consular missions of the United States or diplomatic residences of the United States located in a foreign state. In holding that the SCA did not apply extraterritorially, this Court first noted that the Government conceded that Congress did not intend that the warrant provisions of the SCA to have extraterritorial application.[35]

Secondly, this Court looked to the plain meaning of the SCA itself, and found that no language in the SCA expressly authorized an extraterritorial application capable of overcoming the presumption against extraterritoriality.[36]

Thirdly, this Court rejected the Government's argument that the term "warrant" as used in the SCA was equivalent to a simple subpoena. In doing so, the Court noted that the term warrant was used in the Constitution to protect domestic privacy:

> As the term is used in the Constitution, a warrant is traditionally moored to privacy concepts applied within the territory of the United States:

[35] See *Microsoft* at 210.

[36] *Microsoft* at 21. See also *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247, 130 S.Ct. 2869, 177 L.Ed.2d 535 (2010) for the holding that when Congress intends a law to apply extraterritorially, it gives an "affirmative indication" of that intent.

> "What we know of the history of the drafting of the Fourth Amendment ... suggests that its purpose was to restrict searches and seizures which might be conducted by the United States in domestic matters." *In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157, 169 (2d Cir. 2008) (alteration omitted and ellipses in original) (quoting *United States v. Verdugo-Urquidez*, 494 U.S. 259, 266, 110 S.Ct. 1056, 108 L.Ed.2d 222 (1990)).
>
> Indeed, "if U.S. judicial officers were to issue search warrants intended to have extraterritorial effect, such warrants would have dubious legal significance, if any, in a foreign nation." *Id.* at 171. Accordingly, a warrant protects privacy in a distinctly territorial way.[37]

Finally, the Court found that the SCA's focus was protecting privacy and so an extraterritorial application would be unlawful.[38]

This Court of Appeals' fact-specific analysis not only squares with *Morrison*, but also avoids the sweeping and unwarranted consequences of mandating that any customer relationship that Google maintains with any customer anywhere in the world is necessarily governed by U.S. law.

Congress nowhere indicated that the SCA's warrant provisions should sweep so broadly, and this Court should not adopt such a limitless construction.

---

[37] *Microsoft* at 212-214.

[38] *Microsoft* at 216.

Here, Appellant lived in Italy at all times, making it obvious that his emails and Google Drive files were stored in Google's foreign servers.[39] All emails and information stored in foreign servers were obtained pursuant an unlawful extraterritorial application of the SCA.

The District Court denied Appellant's motion to suppress without a hearing and without giving it any meaningful consideration.

B. The SCA warrant did not authorize the search of and seizure of electronic communications and information stored in servers located outside the U.S.

Even assuming that the SCA warrant could be applied extraterritorially— which this Court of Appeals held that it could not— the warrant itself did not authorize the search of computer servers located abroad. More specifically, the question to be asked is whether the warrant authorizing the search of the "place" described by the warrant, in effect authorized the retrieval of information from offsite severs located outside the U.S. that were accessible by Google.

Looking at the four corners of the SCA warrant the answer is "no," as no such place or method is listed:

> "This warrant applies to information associated with 'gaspolo@gmail.com' that is stored at premises owned, maintained, controlled, or operated by Google, a

[39] Google maintains fifteen data centers around the world, four of which are located in Europe, and nine of which are located in the United States. See https://www.google.com/about/datacenters/inside/locations/index.html (retrieved October 26, 2017).

> company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, CA 94043."

Nowhere in the on the face of the document does the warrant set forth that Google was to search and retrieve information from servers located outside the U.S. This is critical, as historically "warrants" issued by U.S. judges do not run to other countries.

If the Government desired that their warrant apply to all information stored anywhere in the world which had the potential for being retrieved by Google, then this should have been stated directly on the warrant itself as the "place" to be searched.

Accordingly, even assuming an extraterritorial application of the SCA, the seizure of emails stored on foreign computers servers exceeded the scope of the actual SCA warrant used here by the Government, and therefore the foreign stored emails and communications should have been suppressed.

C. Italian Authorities acted as U.S. agents

Evidence obtained by foreign authorities may be suppressed:

> (1) where the conduct of foreign law enforcement officials rendered them agents, or virtual agents, of United States law enforcement officials; or
> (2) where the cooperation between the United States and foreign law enforcement agencies is designed to evade

> constitutional requirements applicable to American officials.[40]

Here, the Italian search warrant was issued upon request of the U.S. government. Appellant was arrested in the Netherlands on a U.S. warrant on or about June 18, 2016. Mr. Pereno testified that he searched Appellant's apartment on July 21, 2016. But after a full year, Mr. Pereno still did not even examine the content of his hard drives.

> Q Mr Pereno, did you review the content of the original hard drives?
>
> A He has done a general forensic review and done a general review of the hard drives but hasn't done it in detail.
> See A-131, 132 ¶¶ 25, 1-3.

The reason is straightforward: in issuing and executing the search warrant, the Italian authorities acted as agents or virtual agents of the U.S. government. This cooperation was designed to evade constitutional requirements applicable to American officials.

If the information sought by the government is stored in a country that has a Mutual Legal Assistance Treaty ("MLAT") with the United States, the government

[40] *United States v. Lee*, 723 F.3d 134, 140 (2d Cir. 2013) citing *United States v. Maturo*, 982 F.2d 57, 61 (2d Cir. 1992).

ordinarily should be required to rely on MLAT procedures, rather than the SCA, to obtain information from a provider's computer systems.

The reason is straightforward. MLAT are binding treaties of the United States, adopted by the President with Senate advice and consent for the precise purpose of addressing the comity concerns (and other logistical obstacles) that cross-border law enforcement investigations frequently present.[41]

When the United States seeks to side-step its own mutually negotiated agreement in favor of unilateral action, it is fair for a court to wonder why, and as such, to adopt a rebuttable presumption that unilateral action under the SCA is inconsistent with international comity principles.

Turning to our case, the United States and Italy have entered into an MLAT Treaty.[42]

Nonetheless, the U.S. government has not even attempted to seize Appellant's email in through an MLAT request and pursuant to Italian law.

In Italy, Appellant would have enjoyed Constitutional rights equivalent to our Fourth and Fifth Amendment, under articles 13 and 14 of the Italian Constitution. But the government made an end run around both countries laws.

[41] See generally, S. Exec. Rep. 110-13, Mutual Legal Assistance Treaties with the European Union, 2-4 (Sept. 11, 2008).
[42] See https://www.state.gov/documents/organization/189224.pdf

VII. THE CONVICTION SHOULD BE REVERSED BECAUSE THE COURT IMPROPERLY ALLOWED SCREENSHOTS FROM THE WAYBACK MACHINE TO BE INTRODUCED AT TRIAL

Before trial, Appellant moved to bar admission of printouts of the Internet archive website, also known as the "Wayback machine." The Court denied the motion.

In *Novak v. Tucows, Inc.*, No. 06-CV-1909, 2007 U.S. Dist. LEXIS 21269 (E.D.N.Y. Mar. 26, 2007), the plaintiff sought to introduce printouts of the Wayback Machine and even provided certifications from the website owner. The Court concluded that the exhibits were, in fact, hearsay, but went on to expound upon the Rule 901 authentication inquiry. The Court held that Plaintiff could not properly authenticate the Internet Archive printouts absent testimony or a sworn statement by an employee of the company that hosted the original version of the site.

To be clear, the Internet site does not host websites, it only takes screenshots of pages that are made available by a website's owner, which can allow or disallow "crawlers" into some, all, or none of the pages of the site.

In *Novak*, the Court opined:

> "While plaintiff's declaration purports to cure his inability to authenticate the documents printed from the internet, he in fact lacks the personal knowledge required to set forth with any certainty that the documents

> obtained via third-party websites are, in fact, what he proclaims them to be.
>
> *This problem is even more acute in the case of documents procured through the Wayback Machine*. Plaintiff states that the web pages archived within the Wayback Machine are based upon "data from third parties who compile the data by using software programs known as crawlers," who then "donate" such data to the Internet Archive, which "preserves and provides access to it." (Novak Decl. P 4.)
>
> Based upon Novak's assertions, it is clear that the information posted on the Wayback Machine is only as valid as the third-party donating the page decides to make it -- the authorized owners and *managers of the archived websites play no role in ensuring that the material posted in the Wayback Machine accurately represents what was posted on their official websites at the relevant time*.
>
> As Novak proffers neither testimony nor sworn statements attesting to the authenticity of the contested web page exhibits by any employee of the companies hosting the sites from which plaintiff printed the pages, such exhibits cannot be authenticated as required under the Rules of Evidence."
> *Id*. at 17-18 (emphasis added).

Notably, this Court of Appeals affirmed the ruling in *Novak*. The panel concluded in an unpublished opinion that "the District Court did not err, much less abuse its discretion" in denying admission of the exhibits.[43]

[43] *Novak v. Tucows Inc.*, 330 F. App'x 204, 204 (2d Cir. 2009).

Here, in denying the motion *in limine*, the District Court ignored *Novak*, citing a few out-of-circuit District Court cases. Besides being not binding in New York, these opinions were not even persuasive. Their analysis failed to consider that the Wayback Machine contained content from at least three different sources, namely:

> (1) web crawlers created and maintained by the Internet Archive;
>
> (2) web crawlers created by Alexa Internet Incorporated, a company owned by Amazon.com; and
>
> (3) web crawlers created and maintained by a variety of third parties that share the results of the crawl with the Internet Archive.

There is no way for a user of the Internet Archive to know whether the retrieved webpage was the result of a web crawler created by the Internet Archive, Alexa Internet, or some unnamed third party.

More importantly, the Internet Archive is not perfect. Sometimes images on webpages show up as blank black boxes, and there are webpages that web crawlers cannot capture either partially or entirely. Thus, no employee of the Internet Archive could possibly establish that records taken from archive.org are true and accurate representations of how relevant websites appeared at relevant times.

Finally, the District Court did not consider that admission of screenshots created by a "crawler," or robots, in a criminal trial, would violate a defendant's rights under the Confrontation Clause.

VIII. THE CONVICTION SHOULD BE REVERSED BECAUSE THE DISTRICT COURT ALLOWED UNAUTHENTICATED HARD DRIVES TO BE INTRODUCED AT TRIAL

At trial, the government's witness, Mr. Pereno testified that he seized hard drives in Appellant's apartment in Rome. Mr. Pereno also testified that he made a copy of the hard drives a month before the trial, and gave it the government.

Appellant objected to the introduction of the copied hard drives at trial for several reasons.

First, Mr. Pereno only took a cursory look at the copied hard drives, and he only relied on the fact that the copies had the same "hash" value of the original. See A-133 ¶¶ 20-24.

A forensic hash is a form of a checksum. A checksum is a mathematical calculation, which in its simplest form, adds up the assorted bits in a data string and provides a value. In other words, a forensic hash is the process of using a mathematical function and applying it to the collected data, which results in a hash value that is a unique identifier for the acquired (collected) data.

A hash value is not a definitive method of authentication. It is like a seal on a bag on controlled substance. Extra files can be planted into the unallocated

section of a hard drive in a virtually undetectable matter. The result would be the same of putting drugs into a bag before sealing it. Mr. Pereno did not provide a full and accurate chain of custody for the hard drives, and therefore he had no way of definitely knowing whether any files had been added to the hard drives in the full year between their seizure and their copy.

More importantly, Mr. Pereno never testified that the computer used to make the copies was in good working conditions. He never testified as to what method he used to create the copy. Was it through an ISO image, or else? We simply don't know.

More importantly, Mr. Pereno never explained what software he used to copy the hard drives, or whether that software was working properly.

Finally, introduction of the copied drives violated the best evidence rule. Neither Mr. Pereno nor any other government witness explained why the original hard drives could not be produced at trial.

IX. THE CONVICTION SHOULD BE REVERSED BECAUSE THE DISTRICT COURT ALLOWED THE GOVERNMENT TO IMPEACH THE ONLY DEFENSE WITNESS WITH A 19-OLD MISDEMEANOR CONVICTION

After the conclusion of the fifth day of trial, the government advised that they intended to impeach the credibility of Kenneth Wong, Appellant's only witness, with a misdemeanor conviction from 1998. Appellant immediately moved the District Court for an order to bar impeachment. See ECF 142.

First, the conviction could not be used under F.R.E. 609(b)(1) because it was older than 10 years and the government failed to set forth specific facts and circumstances showing that the record's probative value *substantially outweighs* its prejudicial effect. Second, F.R.E. 609(b)(2) required the government to give Appellant *reasonable* written notice of the intent to use it. A letter of intent to use such criminal record after the *fifth day of trial* does not meet this standard.

In deciding the issue, the District Court had to consider whether its probative value, supported by specific facts and circumstances, substantially outweighed its prejudicial effect.

This Court of Appeals has recognized that Congress intended that convictions more than ten years old be admitted "very rarely and only in exceptional circumstances."[44]

Nonetheless, the District Court denied Appellant's motion and allowed the government to impeach Mr. Wong with his 19-old conviction.

In *United States v. Ashburn,* the very same District Court had held:

> In this context, the court notes that the Second Circuit has "repeatedly 'recognized that Congress intended that convictions over ten years old be admitted very rarely and only in exceptional circumstances.'" *Farganis*, 397 F.

[44] *Zinman v. Black & Decker, Inc.*, 983 F.2d 431, 434 (2d Cir. 1993); *United States v. Mahler,* 579 F.2d 730, 736 (2d Cir. 1978) (stating that Congress believed that convictions more than ten years old have very little or no probative value); *see also Scotto v. Brady*, 410 F. App'x 355 (2d Cir. 2010); *Farganis v. Town of Montgomery*, 397 F. App'x 666 (2d Cir. 2010).

> App'x at 669 (quoting *Zinman v. Black & Decker (U.S.), Inc.*, 983 F.2d 431, 434 (2d Cir. 1993)).
>
> Yet Ashburn makes no attempt to explain why evidence of Thompson's prior convictions represents one of the exceptional circumstances in which the probative value substantially outweighs its prejudicial effect.[45]

The only difference in this case was that the motion was being made by a *defendant*.

In sum, the was no "exceptional circumstances" justifying admission of a 19-old misdemeanor conviction to impeach the only witness for the defense, and the government should not have been allowed to give notice of impeachment after the fifth day of trial.

X. THE FACTS ESTABLISHED AT TRIAL DO NOT JUSTIFY APPELLANT'S SENTENCE

Appellant was convicted of a single misdemeanor count of obtaining information under 18 U.S.C. 1030. As explained above, the government argued that Appellant created a backdoor into three QNAP devices located in Brooklyn. The government also introduced evidence that Appellant logged into four QNAP devices that were located in Italy and Australia, but there was no evidence that they

[45] *United States v. Ashburn*, No. 11-CR-303 (NGG), 2015 U.S. Dist. LEXIS 115629, at *69 (E.D.N.Y. Aug. 31, 2015)

were "protected computers" or that the access was unauthorized. No commercial purpose or fraudulent intent was ever proven.

More importantly, there was no evidence that Appellant ever set up or operated a botnet. For example, the government argued that Appellant was targeting QNAP devices. All the government witness agreed that the QNAP devices were configured on port 8080. But there was not a shred of evidence that Appellant had even scanned the internet to search for devices on port 8080.

The following is an excerpt of the cross examination of Mr. Cruz:

> Q: Isn't it true that those QNAP devices were port 88[46]?
>
> A: Yes.
>
> Q: Isn't it true that the masscan log that you found related to port 23?
>
> A: Yes
>
> Q: How is the masscan log related to the QNAP?
>
> A: So, I testified and I annotated on my report, that I found these things. I did not attempt to relate these two--particularly the QNAP case. I only testified that I found a log file that showed a scan session of specific IP addresses on port 23.
> See A-125 ¶¶ 14-24.

[46] It should be "on port 8080".

The jury acquitted Appellant of all the felony counts of the indictment, because there was no evidence of wire fraud or fraudulent clicks, much less of money laundering, or intent to defraud.

Nonetheless, the District Court stated that:

> "[b]ased on the evidence that was presented during the course of the trial that it has more than met its obligation of proving by a preponderance of the evidence that all of the factors that were articulated by the Government in its statement now have been met.
>
> In fact, there is substantial documentary and testimonial evidence of the existence of the botnet, of the fraudulent scheme, and of the injury that occurred to individuals, to entities, to Government agencies, and that the defendant engaged in obstruction of justice.
>
> And therefore, the Court agrees with the Government that all of the enhancements that are set forth on page five of the Government's submission have been proven by a preponderance of the evidence."
> See A-25 ¶¶ 6-18.

The District Court determined that the offense level applicable to this misdemeanor conviction was 26. The District Court then imposed a sentence of a year of incarceration, a fine of $100,000 and a year of supervised release. This is the statutory maximum for this offense, and no such sentence was ever before imposed on anyone convicted of a misdemeanor computer intrusion.

There was no evidence at trial to support such a ludicrous sentence. To recap, neither Dr. Ullrich nor Mr. Cruz had seen Appellant operating a botnet. See A-104 ¶¶ 3-19., A-124 ¶¶ 16-21. A witness for the Italian company stated they had no evidence of a single fraudulent click. See A-136 ¶¶ 6-9. The facts presented at trial were, at best, uncorroborated assumptions. The government would have lost the case even in a civil trial using the preponderance of evidence standard.

In the first ever "click fraud" trial, the government did not introduce evidence of a single illegal click. The three QNAP owners that testified at trial could not say whether Appellant had ever accessed their device. None of them testified that they had anything stolen from their device. The government accused Appellant of conspiracy, but no co-conspirator was ever brought to trial.

The "evidence" that District Court referred to was, at best, uncorroborated assumptions. The reality if that the government wanted to prove:

1. The existence of a botnet, with nothing more than an unauthenticated *picture*;
2. The existence of a "click fraud" scheme, without evidence of a *single* fraudulent click to any of Appellant's websites;
3. The existence of a conspiracy, with nothing more than unauthenticated *emails*, and without a *single* alleged coconspirator in court;

4. A Computer Intrusion, without a *single* witness testifying as to when a *single* intrusion would have taken place;
5. An obstruction of justice when, at best, there was no more than an obstruction to *injustice*. The alleged fraudulent business that occurred in Italian against an Italian company was none of the government's business.

For the record, the government called Appellant "a hacker and a thief." See A-103 ¶¶ 19-20. However, the only thing that has been established this far is that Appellant is a *victim* of theft. The government never returned to Appellant his personal property, namely his cellphone, his personal clothes, and his Italian identification card.

The sentence is unconscionable and should be vacated. A Computer Intrusion committed for a non-commercial, non-fraudulent purpose has never led to a year in jail and a fine of $100,000, and there was no reason to make an exception in this case.

The sentence imposed by the District Court is the product of bias. At the time of the jury verdict, Appellant had already served more than the statutory maximum, but the District Court refused to release him.

CONCUSION

For the foregoing reasons, this Court of Appeals should reverse the misdemeanor conviction entered against Appellant. In the alternative, this Court should order that Appellant be given a lower sentence.

Dated: November 16, 2017

Respectfully submitted,

By: */s/ Simone Bertollini*

Simone Bertollini, Esq.
Paul F. O'Reilly, Esq,
Law Offices of Simone Bertollini
450 Seventh Ave, Suite 1408
New York, NY 10123
Tel: (212) 566-3572
Attorneys for Appellant

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, the undersigned counsel hereby certifies as follows:

1. Appellant, Fabio Gasperini is a private party. Therefore, Appellant is not a publicly held corporation, has no parent corporation, and no publicly held corporation owns 10% or more of its stock.

Dated: November 16, 2017 */s/ Simone Bertollini*

CERTIFICATE OF BAR MEMBERSHIP

The undersigned counsel hereby certifies as follows:

1. I am a member in good standing of the bar of the United States Court of Appeals for the Second Circuit.
2. Paul F. O'Reilly is also a member in good standing of the bar of the United States Court of Appeals for the Second Circuit.

Dated: November 16, 2017 */s/ Simone Bertollini*

CERTIFICATE OF IDENTICAL BRIEFS

The undersigned counsel hereby certifies that the text of the electronic and hard copy forms of this brief are identical.

Dated: November 16, 2017 */s/Simone Bertollini*

CERTIFICATE OF VIRUS SCAN

The undersigned counsel hereby certifies as follows:

1. I caused the electronic version of this brief to be checked for computer viruses using ESET NOD 32 8.0.319.0. No computer virus was found.

Dated: November 16, 2017 */s/Simone Bertollini*

CERTIFICATE OF COMPLIANCE

The undersigned counsel hereby certifies as follows:

1. This brief complies with the page limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 10,317 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).
2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in proportionally spaced typeface using Microsoft Word 2013 in 14-point Times New Roman font.

Dated: November 16, 2017 */s/Simone Bertollini*

CERTIFICATE OF SERVICE

The undersigned counsel hereby certifies as follows:

1. The foregoing brief was served upon all counsels of record via the Court's electronic CM/ECF system on November 16, 2017.
2. Six identical hard copies of the foregoing brief, together with six hard copies of the Appendix, will be delivered to the Clerk of the Court on or before November 20, 2017.
3. One identical hard copy of the foregoing brief, together with one hard copy of the Appendix, will be delivered to the counsels for Appellee on or before November 20, 2017.

Dated: November 16, 2017 *<u>/s/Simone Bertollini</u>*

No. 17-2479

In the
United States Court of Appeals
For the Second Circuit

UNITED STATES OF AMERICA,

Appellee,

-v.-

FABIO GASPERINI.

Appellant.

On Appeal from a final judgment of conviction entered by the Hon. Nicholas G. Garaufis, Eastern District of New York

APPELLANT'S APPENDIX

Simone Bertollini, Esq.
Paul F. O'Reilly, Esq.
Law Offices of Simone Bertollini
450 Seventh Ave, Suite 1408
New York, NY 10123
Tel: (212) 566-3572
simone.bertollini@gmail.com

Counsel for Appellant,
Fabio Gasperini

TABLE OF CONTENTS

Page(s)

Criminal Notice of Appeal - Form A

NOTICE OF APPEAL

United States District Court

EASTERN District of NEW YORK

Caption:

UNITED STATES v.

FABIO GASPERINI

Docket No.: 16-CR-441

NICHOLAS G. GARAUFIS
(District Court Judge)

Notice is hereby given that DEFENDANT, FABIO GASPERINI appeals to the United States Court of Appeals for the Second Circuit from the judgment [✓], other [ ] _____ (specify)

entered in this action on 08/04/2017 (date).

This appeal concerns: Conviction only [ ] Sentence only [ ] Conviction & Sentence [✓] Other [ ]

Defendant found guilty by plea [ ] trial [✓] N/A [ ]

Offense occurred after November 1, 1987? Yes [✓] No [ ] N/A [ ]

Date of sentence: _____ N/A [✓]

Bail/Jail Disposition: Committed [✓] Not committed [ ] N/A [ ]

Appellant is represented by counsel? Yes [✓] No [ ] If yes, provide the following information:

Defendant's Counsel: SIMONE BERTOLLINI

Counsel's Address: 450 SEVENTH AVENUE, SUITE 1408

NEW YORK, NY 10123

Counsel's Phone: (212) 566-3572

Assistant U.S. Attorney: SARITHA KOMATIREDDY

AUSA's Address: 271 CADMAN PLAZA EAST

BROOKLYN, NY 11201

AUSA's Phone: (718) 254-6054

Simone Bertollini
Signature

CLOSED,APPEAL,CUSTAPP

U.S. District Court
Eastern District of New York (Brooklyn)
CRIMINAL DOCKET FOR CASE #: 1:16−cr−00441−NGG All Defendants

Case title: USA v. Gasperini

Date Filed: 08/04/2016
Date Terminated: 08/11/2017

Assigned to: Judge Nicholas G. Garaufis

Defendant (1)

Fabio Gasperini
TERMINATED: 08/11/2017

represented by **Simone Bertollini**
Law Office of Simone Bertollini
450 Seventh Avenue
Suite 1408
New York, NY 10123
212−566−3572
Fax: 917−512−4400
Email: simone.bertollini@gmail.com
ATTORNEY TO BE NOTICED
Designation: Retained

Pending Counts	**Disposition**
18, United States Code, Sections 1030(a)(4), 1030(b), 1030(c)(3)(A), 2 and 3551 et seq− COMPUTER INTRUSION (2)	Receives 12 months imprisonment; 1 year supervised release with special condition − compliance with Forfeiture Order to be filed within 90 days; $25.00 Assessment; $100,000 Fine

Highest Offense Level (Opening)

Felony

Terminated Counts	**Disposition**
18, United States Code, Sections 1030(a)(4), 1030(b), 1030(c)(3)(A), 2 and 3551 et seq− COMPUTER INTRUSION (1)	Found Not Guilty by Jury Verdict
18, United States Code, Sections 1349 and 3551 et seq− WIRE FRAUD CONSPIRACY (3)	Found Not Guilty by Jury Verdict
18, United States Code, Sections 1343, 2 and 3551 et seq− WIRE FRAUD (4)	Found Not Guilty by Jury Verdict
18, United States Code, Sections 1956(h) and 3551 et seq− MONEY LAUNDERING CONSPIRACY (5)	Found Not Guilty by Jury Verdict

Highest Offense Level (Terminated)

Felony

Complaints	**Disposition**
18 USC 1030(a)(4)	

Interested Party

Linode, LLC represented by **Lynn E. Judell**
Schwartz Sladkus Reich Greenberg Atlas, LLP
270 Madison Avenue
New York, NY 10016
212−743−7000
Fax: 212−743−7001
Email: ljudell@ssrga.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED
Designation: Retained

Peter Fu
Cooper Levenson, P.A.
1125 Atlantic Avenue
Third Floor
Atlantic City, NJ 08401
609−572−7556
Fax: 609−572−7557
Email: pfu@cooperlevenson.com
ATTORNEY TO BE NOTICED

Plaintiff

USA represented by **Saritha Komatireddy**
US Attorney's Office − EDNY
271 Cadman Plaza East
Brooklyn, NY 11201
718−254−6054
Fax: 718−254−6076
Email: saritha.komatireddy@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED
Designation: Government Attorney

Melody Wells
United States Attorney's Office − EDNY
271 Cadman Plaza East
Brooklyn, NY 11201
718−254−6422
Fax: 718−254−6076
Email: melody.wells@usdoj.gov
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
08/14/2015	1	SEALED COMPLAINT and affidavit in support of arrest warrant as to Fabio Gasperini (1). (Yuen, Sui−May) [1:15−mj−00769−LB *SEALED*] (Entered: 08/17/2015)
08/04/2016	3	SEALED INDICTMENT as to Fabio Gasperini (1) count(s) 1−2, 3, 4, 5. (Attachments: # 1 Criminal Information Sheet, # 2 Sealing Cover Sheet) (Manson, Eddie) (Entered: 08/09/2016)

08/04/2016	5	Limited Sealing Order is granted as to Fabio Gasperini. So Ordered by Magistrate Judge Steven M. Gold on 8/4/2016. (Attachments: # 1 Application) (Manson, Eddie) (Entered: 08/09/2016)
03/07/2017	6	NOTICE OF ATTORNEY APPEARANCE: Simone Bertollini appearing for Fabio Gasperini. (Lee, Tiffeny) (Entered: 03/08/2017)
04/21/2017	7	Order to Unseal the Above Captioned Case as to Fabio Gasperini.. So Ordered by Magistrate Judge Peggy Kuo on 4/21/2017. (Lee, Tiffeny) (Entered: 04/24/2017)
04/21/2017	14	Minute Entry for proceedings held before Magistrate Judge Peggy Kuo:Arraignment as to Fabio Gasperini (1) Count 1−2,3,4,5 held on 4/21/2017. Counsel for parties present. Plea entered by Fabio Gasperini Not Guilty on ALL COUNTS. (Temporary Order of Detention Issued. Bail Hearing set for 4/25/2017 11:00 AM. (Tape #2:50−2:57.) (Almonte, Giselle) Modified to include preliminary hearing waived on 4/27/2017 (Almonte, Giselle). (Entered: 04/27/2017)
04/21/2017	15	ORDER OF TEMPORARY DETENTION PENDING HEARING PURSUANT TO BAIL REFORM ACT as to Fabio Gasperini. Detention Hearing set for 4/25/2017 11:00 AM before Duty Magistrate Judge. Ordered by Magistrate Judge Peggy Kuo on 4/21/2017. (Almonte, Giselle) (Entered: 04/27/2017)
04/24/2017	8	NOTICE of Change of address by Fabio Gasperini (Bertollini, Simone) (Entered: 04/24/2017)
04/24/2017	9	MOTION to Dismiss *Indictment* by Fabio Gasperini. (Attachments: # 1 Notice of Motion Letter to the Court) (Bertollini, Simone) (Entered: 04/24/2017)
04/25/2017		Minute Entry for proceedings held before Judge Nicholas G. Garaufis: Status Conference held on 4/25/2017. Counsel for all parties present. The court set the following briefing schedule for Defendant's motion to dismiss, filed on April 24, 2017: The Government shall serve its response by no later than May 8, 2015; and Defendant shall serve his reply, if any, and file the fully briefed motion by no later than May 15, 2017. Oral argument on the motion is scheduled for May 25, 2017, at 9:00 AM in Courtroom 4D South. Time is excluded under the Speedy Trial Act between 4/24/2017 nunc pro tunc and 5/25/2017, in the interest of justice for review of the motion to dismiss and discovery on consent of the parties. (Court Reporter Georgette Betts) (Interpreter Maria Galetta) (Houlihan, Michael) (Entered: 04/25/2017)
04/25/2017	16	Minute Entry for proceedings held before Magistrate Judge Steven Tiscione: Detention Hearing as to Fabio Gasperini held on 4/25/2017. Counsel for all parties present. Defense Counsel request defendant's release on R.O.R for reasons stated on the record. Government opposed. Court denied R.O.R request, finds defendant a risk of flight. Order of detention entered w/o prejudice. (Tape #11:24−11:49.) (Almonte, Giselle) (Entered: 04/28/2017)
04/25/2017	17	ORDER OF DETENTION PENDING TRIAL as to Fabio Gasperini. So Ordered by Magistrate Judge Steven Tiscione on 4/25/2017. (Almonte, Giselle) (Entered: 04/28/2017)
04/26/2017	10	Letter *to U.S. Attorney Requesting Discovery* as to Fabio Gasperini (Bertollini, Simone) (Entered: 04/26/2017)
04/26/2017	11	TRANSCRIPT of Proceedings as to Fabio Gasperini held on April 21, 2017, before Judge Kuo. Court Reporter/Transcriber TypeWrite Word Processing Service, Telephone number 518−581−8973. Email address: transcripts@typewp.com. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER.File redaction request using event "Redaction Request − Transcript" located under "Other Filings − Other Documents". Redaction Request due 5/17/2017. Redacted Transcript Deadline set for 5/29/2017. Release of Transcript Restriction set for 7/25/2017. (Hong, Loan) (Entered: 04/26/2017)
04/26/2017	12	NOTICE OF ATTORNEY APPEARANCE Melody Wells appearing for USA. (Wells, Melody) (Entered: 04/26/2017)

04/27/2017	13	MOTION to Modify Conditions of Release *and Revoke Pretrial Detention Order* by Fabio Gasperini. (Attachments: # 1 Memorandum in Support) (Bertollini, Simone) (Entered: 04/27/2017)
04/28/2017	18	MOTION for Protective Order *for Sensitive Discovery Materials* by USA as to Fabio Gasperini. (Attachments: # 1 Proposed Order) (Komatireddy, Saritha) (Entered: 04/28/2017)
04/29/2017	19	MEMORANDUM in Opposition re 18 MOTION for Protective Order *for Sensitive Discovery Materials* (Bertollini, Simone) (Entered: 04/29/2017)
05/01/2017		ORDER re Defendant's 13 Motion to Modify Conditions of Release. The Government shall file its response to the Motion by no later than May 3, 2017. The court will hold a Detention Hearing on May 5, 2017, at 2:00 PM in courtroom 4D South. Ordered by Judge Nicholas G. Garaufis on 05/01/2017. (Houlihan, Michael) (Entered: 05/01/2017)
05/01/2017		ORDER re Government's 18 Motion for Protective Order. The Government shall file its response to Defendant's 19 Memorandum in Opposition to the Motion by no later than May 5, 2017. Ordered by Judge Nicholas G. Garaufis on 5/1/2017. (Houlihan, Michael) (Entered: 05/01/2017)
05/03/2017	20	TRANSCRIPT of Proceedings as to Fabio Gasperini held on April 25, 2017, before Judge TISCIONE. Court Reporter/Transcriber TypeWrite Word Processing Service, Telephone number 518−581−8973. Email address: transcripts@typewp.com. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER.File redaction request using event "Redaction Request − Transcript" located under "Other Filings − Other Documents". Redaction Request due 5/24/2017. Redacted Transcript Deadline set for 6/5/2017. Release of Transcript Restriction set for 8/1/2017. (Hong, Loan) (Entered: 05/03/2017)
05/03/2017	21	RESPONSE in Opposition re 13 MOTION to Modify Conditions of Release *and Revoke Pretrial Detention Order* (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit C, # 4 Exhibit D) (Komatireddy, Saritha) (Entered: 05/03/2017)
05/05/2017	22	REPLY TO RESPONSE to Motion re 18 MOTION for Protective Order *for Sensitive Discovery Materials* (Komatireddy, Saritha) (Entered: 05/05/2017)
05/05/2017		Minute Entry for proceedings held before Judge Nicholas G. Garaufis: Detention Hearing held on 05/05/2017. Counsel for all parties present. The court denied Defendant's 13 Motion to Modify Conditions of Release and ordered Defendant to be detained pending trial. Jury selection and trial is scheduled for July 24, 2017. (Court Reporter Holly Driscoll) (Interpreter Sandra Borri) (Houlihan, Michael) (Entered: 05/05/2017)
05/05/2017	25	ORDER OF DETENTION as to Fabio Gasperini. So Ordered by Judge Nicholas G. Garaufis on 5/5/2017. (Lee, Tiffeny) (Entered: 05/08/2017)
05/05/2017	26	ORDER granting 18 Motion for Protective Order as to Fabio Gasperini (1). So Ordered by Judge Nicholas G. Garaufis on 5/5/2017. (Lee, Tiffeny) (Entered: 05/08/2017)
05/06/2017	23	Letter *from the government to defense counsel regarding discovery* as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 05/06/2017)
05/08/2017	24	NOTICE *of Intent to File Motion for a Bill of Particulars* as to Fabio Gasperini (Bertollini, Simone) (Entered: 05/08/2017)
05/08/2017	27	MEMORANDUM in Opposition re 9 MOTION to Dismiss *Indictment* (Attachments: # 1 Exhibit A) (Wells, Melody) (Entered: 05/08/2017)
05/08/2017	28	Letter *re Notice of Motion for Bill of Particulars ECF No. 24* as to Fabio Gasperini (Wells, Melody) (Entered: 05/08/2017)
05/09/2017	29	NOTICE *of Request of pre−motion conference* as to Fabio Gasperini (Attachments: # 1 Exhibit A, # 2 Exhibit B) (Bertollini, Simone) (Entered: 05/09/2017)
05/10/2017		ORDER re Defendant's 29 Application for a Pre−Motion Conference. The Application is GRANTED. The parties are instructed to confer and contact the court's Deputy at

		718−613−2545 to schedule the pre−motion conference. Ordered by Judge Nicholas G. Garaufis on 5/10/2017. (Houlihan, Michael) (Entered: 05/10/2017)
05/11/2017	30	REPLY TO RESPONSE to Motion re 9 MOTION to Dismiss *Indictment* (Bertollini, Simone) (Entered: 05/11/2017)
05/12/2017	31	NOTICE OF APPEAL of Conditions of Release by Fabio Gasperini as to 25 Order of Detention Filing fee $ 505, receipt number 0207−9523772. (Attachments: # 1 Appendix Transcripts, # 2 Criminal Appeal Transcript Information − Form B) (Bertollini, Simone) (Entered: 05/12/2017)
05/12/2017		Electronic Index to Record on Appeal as to Fabio Gasperini sent to US Court of Appeals 31 Notice of Appeal − Conditions of Release, Documents are available via Pacer. For docket entries without a hyperlink or for documents under seal, contact the court and we'll arrange for the document(s) to be made available to you. (McGee, Mary Ann) (Entered: 05/12/2017)
05/17/2017	33	Letter *regarding May 18, 2017 status conference* as to Fabio Gasperini (Wells, Melody) (Entered: 05/17/2017)
05/19/2017	35	MOTION for Disclosure *of Grand Jury Transcripts under FRCP 6(e)(3)(E)(i)* by Fabio Gasperini. (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit C) (Bertollini, Simone) (Entered: 05/19/2017)
05/19/2017	36	MOTION for Bill of Particulars by Fabio Gasperini. (Bertollini, Simone) (Entered: 05/19/2017)
05/19/2017	37	NOTICE as to Fabio Gasperini re 35 MOTION for Disclosure *of Grand Jury Transcripts under FRCP 6(e)(3)(E)(i)* (Bertollini, Simone) (Entered: 05/19/2017)
05/22/2017		Minute Entry for proceedings held before Judge Nicholas G. Garaufis: Status Conference held on 5/18/2017. The court GRANTED Defendant leave to file a motion for a bill of particulars. The court set the following briefing schedule for Defendant's motions for a bill of particulars and to compel production of grand jury testimony: Defendant shall serve his combined motions by May 19, 2017; and the Government shall serve its response and file the fully briefed motions by May 23, 2017. Oral argument on those motions and Defendant's pending motion to dismiss is scheduled for May 25, 2017, at 3:00 PM in Courtroom 4D South. The court also set the following briefing schedule for Defendant's proposed motion to suppress: Defendant shall serve his motion on June 16, 2017; the Government shall serve its response on June 30, 2017; and Defendant shall serve his reply, if any, and file the fully briefed motion on July 7, 2017. Oral argument on the motion is scheduled for July 13, 2017, at 11:00 AM in Courtroom 4D South. (Court Reporter Lisa Schmid) (Interpreter Sandra Borri) (Houlihan, Michael) (Entered: 05/22/2017)
05/23/2017	38	Letter *re expert witnesses* as to Fabio Gasperini (Wells, Melody) (Entered: 05/23/2017)
05/23/2017	39	MEMORANDUM in Opposition re 35 MOTION for Disclosure *of Grand Jury Transcripts under FRCP 6(e)(3)(E)(i)*, 36 MOTION for Bill of Particulars (Wells, Melody) (Entered: 05/23/2017)
05/24/2017	40	REPLY TO RESPONSE to Motion re 36 MOTION for Bill of Particulars (Bertollini, Simone) (Entered: 05/24/2017)
05/24/2017	41	REPLY TO RESPONSE to Motion re 35 MOTION for Disclosure *of Grand Jury Transcripts under FRCP 6(e)(3)(E)(i)* (Bertollini, Simone) (Entered: 05/24/2017)
05/25/2017	42	Letter *from the government to defense counsel regarding discovery* as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 05/25/2017)
05/25/2017		Minute Entry for proceedings held before Judge Nicholas G. Garaufis: Oral Argument held on 05/25/2017 re Defendant Fabio Gasperini's 9 Motion to Dismiss, 35 Motion for Disclosure of Grand Jury Transcripts, and 36 Motion for a Bill of Particulars. The court reserved decision on the Defendant's motions. By operation of law, time is excluded under the Speedy Trial Act until the court issues its decision on Defendant's motions. (Court Reporter Richard Barry) (Interpreter Sandra Borri) (Houlihan,

		Michael) (Entered: 05/25/2017)
05/26/2017	43	Letter *from the government to defense counsel regarding discovery* as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 05/26/2017)
05/31/2017	44	Letter as to Fabio Gasperini (Bertollini, Simone) (Entered: 05/31/2017)
06/01/2017	45	MEMORANDUM & ORDER, For the foregoing reasons, Defendant's 9 and 35 motions to dismiss the indictment and for disclosure of grand jury materials are DENIED WITHOUT PREJUDICE, and his 36 motion for a bill of particulars is GRANTED IN PART and DENIED IN PART. The Government is ORDERED to provide Defendant with a bill of particulars identifying the categories of information alleged to have been "obtained" in connection with the Counts One and Two of the Indictment by no later than June 9, 2017. So Ordered by Judge Nicholas G. Garaufis on 5/31/2017. (Lee, Tiffeny) (Entered: 06/01/2017)
06/05/2017	46	First MOTION for Extension of Time to File *Motion in limine to exclude evidence* by Fabio Gasperini. (Attachments: # 1 Proposed Order) (Bertollini, Simone) (Entered: 06/05/2017)
06/05/2017		ORDER re Defendant's 46 Motion for Extension of Time to File: Defendant is DIRECTED to submit a revised proposed order with a full briefing schedule that includes the Government's response and Defendant's reply, if any. Ordered by Judge Nicholas G. Garaufis on 6/5/2017. (Houlihan, Michael) (Entered: 06/05/2017)
06/06/2017	47	NOTICE *Revised Proposed Order* as to Fabio Gasperini re 46 First MOTION for Extension of Time to File *Motion in limine to exclude evidence* (Bertollini, Simone) (Entered: 06/06/2017)
06/06/2017	48	Letter *Requesting Discovery* as to Fabio Gasperini (Bertollini, Simone) (Entered: 06/06/2017)
06/06/2017	49	Letter *regarding discovery* as to Fabio Gasperini (Wells, Melody) (Entered: 06/06/2017)
06/07/2017	50	Letter *from the government to defense counsel regarding discovery* as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 06/07/2017)
06/09/2017	51	Letter *from the government to defense counsel regarding meetings at the MDC* as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 06/09/2017)
06/09/2017	52	ORDER re 46 Motion for Extension of Time to File as to Fabio Gasperini (1). Defendant is allowed to file his Motion in limine to exclude evidence on or before June 27, 2017. The Government's response shall be filed on or before July 11, 2017. Defendant's reply, if any, shall be filed on or before July 12, 2017. So Ordered by Judge Nicholas G. Garaufis on 6/6/2017. (Lee, Tiffeny) (Entered: 06/09/2017)
06/09/2017	53	Letter *Providing a Bill of Particulars Regarding the Categories of Information Obtained* as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 06/09/2017)
06/12/2017	54	Letter *Requesting discovery* as to Fabio Gasperini (Bertollini, Simone) (Entered: 06/12/2017)
06/14/2017	55	Letter *Requesting Discovery* as to Fabio Gasperini (Bertollini, Simone) (Entered: 06/14/2017)
06/14/2017	56	Letter *from the government to defense counsel regarding discovery* as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 06/14/2017)
06/16/2017	57	Letter *from the government to defense counsel regarding discovery* as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 06/16/2017)
06/16/2017	58	Second MOTION to Dismiss *Indictment* by Fabio Gasperini. (Attachments: # 1 Notice of Motion Letter to the Court) (Bertollini, Simone) (Entered: 06/16/2017)
06/16/2017	59	MOTION to Suppress *Evidence* by Fabio Gasperini. (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit C, # 4 Exhibit D, # 5 Exhibit E) (Bertollini, Simone) (Entered: 06/16/2017)

06/17/2017	60	MEMORANDUM in Support re 58 Second MOTION to Dismiss *Indictment or for alternative relief* (Bertollini, Simone) (Entered: 06/17/2017)
06/19/2017	61	MOTION to Compel *Discovery* by Fabio Gasperini. (Bertollini, Simone) (Entered: 06/19/2017)
06/20/2017		ORDER re Defendant's 58 Second Motion to Dismiss the Indictment and 61 Motion to Compel Discovery. The Government is DIRECTED to file its response to Defendant's Motions by no later than June 30, 2017. Ordered by Judge Nicholas G. Garaufis on 06/20/2017. No reply shall be permitted. (Houlihan, Michael) (Entered: 06/20/2017)
06/20/2017	62	NOTICE OF FILING OF OFFICIAL TRANSCRIPT of Proceedings as to Fabio Gasperini held on 5/25/2017, before Judge NICHOLAS G. GARAUFIS. Court Reporter/Transcriber Richard W. Barry, Telephone number 718−613−2505. Email address: rwbarrycourtreporter@gmail.com. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER.File redaction request using event "Redaction Request − Transcript" located under "Other Filings − Other Documents". Redaction Request due 7/11/2017. Redacted Transcript Deadline set for 7/21/2017. Release of Transcript Restriction set for 9/18/2017. (Barry, Richard) (Entered: 06/20/2017)
06/20/2017	63	Letter *from the government to defense counsel regarding discovery* as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 06/20/2017)
06/21/2017	64	Letter *from the government to defense counsel regarding visiting the MDC* as to Fabio Gasperini (Attachments: # 1 MDC Brooklyn Computer Laptop and External Hard Drive Form) (Komatireddy, Saritha) (Entered: 06/21/2017)
06/26/2017	65	MOTION in Limine *to Exclude Evidence* by Fabio Gasperini. (Attachments: # 1 Exhibit A) (Bertollini, Simone) (Entered: 06/26/2017)
06/26/2017		NOTICE OF HEARING as to Fabio Gasperini: This case has been referred to me for selection of a trial jury on July 24, 2017. Counsel must appear promptly at 9:00 AM that day in Courtroom 4D South to begin selection. The parties must submit no later than noon on July 14, 2017 the following (to the extent not previously submitted): proposed questions to ask prospective jurors during voir dire, a short description of the case and a list of the names of all persons, entities, and locations that the party expects may be mentioned during the trial. Only questions specifically addressing the issues to be tried should be submitted; routine background questions are not necessary. Ordered by Magistrate Judge Vera M. Scanlon on 6/26/2017 (Quinlan, Krista) (Entered: 06/26/2017)
06/27/2017	66	Letter *from the government to defense counsel regarding discovery* as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 06/27/2017)
06/30/2017	68	MEMORANDUM in Opposition re 58 Second MOTION to Dismiss *Indictment and 60 Memorandum ISO Second Motion to Dismiss* (Attachments: # 1 Exhibit C, # 2 Exhibit D, # 3 Exhibit E, # 4 Exhibit F) (Wells, Melody) (Entered: 06/30/2017)
06/30/2017	69	MEMORANDUM in Opposition re 58 Second MOTION to Dismiss *Indictment and 60 Memorandum ISO Second Motion to Dismiss enclosing Exhibits A and B* (Attachments: # 1 Exhibit) (Wells, Melody) (Entered: 06/30/2017)
06/30/2017	81	NOTICE OF ATTORNEY APPEARANCE: Lynn E. Judell appearing for Linode, LLC. (Lee, Tiffeny) (Entered: 07/07/2017)
06/30/2017	82	MOTION to Quash *Subpoena to Testify* by Linode, LLC as to Fabio Gasperini. (Attachments: # 1 Exhibits, # 2 Cover Letter) (Lee, Tiffeny) (Entered: 07/07/2017)
07/01/2017	70	MEMORANDUM in Opposition re 61 MOTION to Compel *Discovery* (Wells, Melody) (Entered: 07/01/2017)
07/01/2017	71	MEMORANDUM in Opposition re 59 MOTION to Suppress *Evidence* (Attachments: # 1 Exhibit A, # 2 Exhibit B) (Komatireddy, Saritha) (Entered: 07/01/2017)
07/01/2017	72	Letter *from the government to defense counsel regarding discovery* as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 07/01/2017)

07/01/2017	73	Letter *to the Court* as to Fabio Gasperini (Bertollini, Simone) (Entered: 07/01/2017)
07/03/2017	74	REPLY TO RESPONSE to Motion re 61 MOTION to Compel *Discovery* (Bertollini, Simone) (Entered: 07/03/2017)
07/03/2017	75	REPLY TO RESPONSE to Motion re 61 MOTION to Compel *Discovery enclosing Exhibit A* (Bertollini, Simone) (Entered: 07/03/2017)
07/05/2017	76	Letter *from the government to defense counsel regarding discovery* as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 07/05/2017)
07/06/2017	77	Letter *to prosecutor regarding discovery* as to Fabio Gasperini (Bertollini, Simone) (Entered: 07/06/2017)
07/06/2017	78	REPLY TO RESPONSE to Motion re 59 MOTION to Suppress *Evidence* (Attachments: # 1 Exhibit A) (Bertollini, Simone) (Entered: 07/06/2017)
07/06/2017	79	NOTICE OF FILING OF OFFICIAL TRANSCRIPT of Proceedings as to Fabio Gasperini held on April 25, 2017, before Judge Nicholas G. Garaufis. Court Reporter/Transcriber Georgette K. Betts, Telephone number 718−804−2777. Email address: Georgette_Betts@nyed.uscourts.gov. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER.File redaction request using event "Redaction Request − Transcript" located under "Other Filings − Other Documents". Redaction Request due 7/27/2017. Redacted Transcript Deadline set for 8/7/2017. Release of Transcript Restriction set for 10/4/2017. (Betts, Georgette) (Entered: 07/06/2017)
07/06/2017	80	Letter *to the Court opposing exclusion of evidence and continuance of trial date, and seeking preclusion of defense argument* as to Fabio Gasperini (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit C) (Komatireddy, Saritha) Modified to motion on 7/20/2017 (Lee, Tiffeny). (Entered: 07/06/2017)
07/07/2017		Minute Entry for proceedings held before Judge Nicholas G. Garaufis: Status Conference held on 07/06/2017. Counsel for all parties present. The court DENIED Defendant's 58 Second Motion to Dismiss and 61 Motion to Compel. The parties consented to have jury selection conducted by a magistrate judge. (Court Reporter Linda Danelczyk) (Interpreter Maria Galetta) (Houlihan, Michael) (Entered: 07/07/2017)
07/07/2017	83	Letter *to the prosecutor regarding Defendant's access to discovery* as to Fabio Gasperini (Bertollini, Simone) (Entered: 07/07/2017)
07/07/2017	84	Letter *from the government to defense counsel regarding discovery* as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 07/07/2017)
07/09/2017	85	RESPONSE in Opposition re 59 MOTION to Suppress *Evidence − Letter Supplementing the Record* (Attachments: # 1 Exhibit C, # 2 Exhibit D) (Komatireddy, Saritha) (Entered: 07/09/2017)
07/10/2017	86	ORDER as to Fabio Gasperini : On June 30, 2017, non−party Linode, LLC's ("Linode") filed a motion to quash a subpoena ad testificandum issued in connection with the above−captioned action. (Mot. to Quash (Dkt. 82).) Linode is ORDERED to appear before the court on 7/13/2017 at 11:00 AM in Courtroom 4D South before Judge Nicholas G. Garaufis. At that time, the court will hear from Linode, as well as the Government and Defendant Fabio Gasperini, regarding the merits of Linode's motion to quash. So Ordered by Judge Nicholas G. Garaufis on 7/10/2017. (Lee, Tiffeny) (Entered: 07/10/2017)
07/10/2017	87	REPLY TO RESPONSE to Motion re 59 MOTION to Suppress *Evidence* (Bertollini, Simone) (Entered: 07/10/2017)
07/10/2017	88	Letter *from the government to defense counsel regarding discovery* as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 07/10/2017)
07/11/2017	89	MOTION to Quash by Linode, LLC as to Fabio Gasperini. (Judell, Lynn) (Entered: 07/11/2017)

07/11/2017	90	Proposed Jury Instructions by Fabio Gasperini (Attachments: # 1 Proposed Verdict Sheet) (Bertollini, Simone) (Entered: 07/11/2017)
07/11/2017	91	WITNESS LIST by Fabio Gasperini (Bertollini, Simone) (Entered: 07/11/2017)
07/11/2017		ORDER re Non−Party Linode LLC's 89 Application to adjourn the hearing on Linode's 82 motion to quash. The Application is GRANTED. Linode is DIRECTED to confer with the parties and contact the court's Deputy at (718) 613−2545 to reschedule the hearing. The oral argument currently scheduled for July 13, 2017, at 11:00 AM is unaffected by this order and will proceed as scheduled. Ordered by Judge Nicholas G. Garaufis on 7/11/2017. (Houlihan, Michael) (Entered: 07/11/2017)
07/11/2017	92	RESPONSE to Motion re 89 MOTION to Quash , 82 MOTION to Quash *Subpoena to Testify* (Bertollini, Simone) (Entered: 07/11/2017)
07/11/2017	93	RESPONSE in Opposition re 65 MOTION in Limine *to Exclude Evidence* (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit D) (Komatireddy, Saritha) (Entered: 07/11/2017)
07/11/2017	94	RESPONSE in Opposition re 65 MOTION in Limine *to Exclude Evidence Exhibit C (filed under seal)* (Komatireddy, Saritha) (Entered: 07/11/2017)
07/12/2017	95	Proposed Voir Dire by Fabio Gasperini (Bertollini, Simone) (Entered: 07/12/2017)
07/12/2017	96	NOTICE OF FILING OF OFFICIAL TRANSCRIPT of Proceedings as to Fabio Gasperini held on July 6, 2017, before Judge Nicholas G. Garaufis. Court Reporter/Transcriber Linda Danelczyk, Telephone number 718−613−2330. Email address: linda_danelczyk@nyed.uscourts.gov. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER.File redaction request using event "Redaction Request − Transcript" located under "Other Filings − Other Documents". Redaction Request due 8/2/2017. Redacted Transcript Deadline set for 8/14/2017. Release of Transcript Restriction set for 10/10/2017. (Danelczyk, Linda) (Entered: 07/12/2017)
07/12/2017	97	REPLY TO RESPONSE to Motion re 65 MOTION in Limine *to Exclude Evidence* (Bertollini, Simone) (Entered: 07/12/2017)
07/12/2017	98	ORDER as to Fabio Gasperini re 92 Response to Motion/Defendant's request to be exempted from participating in the hearing re Linode's Motion to Quash. Application granted. So Ordered by Judge Nicholas G. Garaufis on 7/12/2017. (Lee, Tiffeny) (Entered: 07/12/2017)
07/12/2017	99	Proposed Jury Instructions by USA as to Fabio Gasperini (Attachments: # 1 Proposed Verdict Sheet) (Komatireddy, Saritha) (Entered: 07/12/2017)
07/13/2017		ORDER re the Government's 80 Letter seeking preclusion of defense argument. The Government is ORDERED to provide supplemental briefing stating clearly the legal basis for its motion to preclude Defendant from arguing that the Government forged documents produced in discovery and from calling one of the prosecutors as a trial witness. The Government's brief shall not exceed five pages, and shall be submitted by July 14, 2017. Defendant may respond to the Government's arguments, in a brief not to exceed five pages, by July 17, 2017. Ordered by Judge Nicholas G. Garaufis on 07/13/2017. (Houlihan, Michael) (Entered: 07/13/2017)
07/13/2017		Minute Entry for proceedings held before Judge Nicholas G. Garaufis: Oral Argument held on 07/13/2017 re Defendant Fabio Gasperini's 59 motion to suppress. Counsel for all parties present. The court reserved decision on the Defendant's motion. (Court Reporter Anthony Mancuso) (Interpreter Maria Galetta) (Houlihan, Michael) (Entered: 07/13/2017)
07/13/2017	100	First MOTION for Leave to Appear Pro Hac Vice *for Peter Fu* Filing fee $ 150, receipt number 0207−9677519.by Linode, LLC as to Fabio Gasperini. (Attachments: # 1 Notice of Motion, # 2 Admission Information) (Fu, Peter) (Entered: 07/13/2017)
07/13/2017	101	Proposed Voir Dire by USA as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 07/13/2017)

07/14/2017	102	Letter *to prosecutor regarding expert disclosures* as to Fabio Gasperini (Bertollini, Simone) (Entered: 07/14/2017)
07/14/2017	103	Letter *to prosecutor regarding defense exhibit list* as to Fabio Gasperini (Bertollini, Simone) (Entered: 07/14/2017)
07/14/2017	104	Letter *from the government with a short description of the case for use during jury selection* as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 07/14/2017)
07/14/2017	105	Second MOTION in Limine *to Bar Introduction of Evidence* by Fabio Gasperini. (Bertollini, Simone) (Entered: 07/14/2017)
07/14/2017	106	Letter *from the government regarding 18 U.S.C. 3500 Material* as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 07/14/2017)
07/14/2017	107	Letter *in further support of motion to preclude* as to Fabio Gasperini (Wells, Melody) (Entered: 07/14/2017)
07/14/2017	108	MOTION to Produce *summary of expert opinion* by USA as to Fabio Gasperini. (Wells, Melody) (Entered: 07/14/2017)
07/14/2017	109	WITNESS LIST by USA as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 07/14/2017)
07/14/2017	110	RESPONSE to Motion re 108 MOTION to Produce *summary of expert opinion* (Bertollini, Simone) (Entered: 07/14/2017)
07/14/2017	111	Third MOTION in Limine *to Exclude Business Certifications* by Fabio Gasperini. (Bertollini, Simone) (Entered: 07/14/2017)
07/14/2017	112	EXHIBIT LIST by USA as to Fabio Gasperini (Attachments: # 1 Exhibit) (Wells, Melody) (Entered: 07/14/2017)
07/15/2017	114	Letter *regarding discovery* as to Fabio Gasperini (Wells, Melody) (Entered: 07/15/2017)
07/17/2017	115	Letter *in further opposition of motion to preclude* as to Fabio Gasperini (Bertollini, Simone) (Entered: 07/17/2017)
07/17/2017	116	MEMORANDUM & ORDER denying 59 Motion to Suppress as to Fabio Gasperini (1). So Ordered by Judge Nicholas G. Garaufis on 7/13/2017. (Lee, Tiffeny) (Entered: 07/17/2017)
07/17/2017		ORDER re the Government's 108 motion to compel Defendant to provide a summary of expert testimony. The motion is GRANTED. On May 23, 2017, the Government provided a copy of its proposed expert testimony pursuant to Federal Rule of Criminal Procedure 16(a)(1)(G). (See May 23, 2017, Ltr. (Dkt. 38).) This disclosure was sufficient to trigger Defendant's mutual discovery obligations. See Rule 16(b)(1)(C)(ii) ("The defendant must, at the government's request, give to the government a written summary of any [proposed expert testimony] the defendant intends to use... as evidence at trial, if... the defendant requests disclosure under subdivision (a)(1)(G) and the government complies.") Defendant is DIRECTED to provide a summary of proposed expert testimony to the Government by no later than July 19, 2017. So ordered by Judge Nicholas G. Garaufis on 07/17/2017. (Houlihan, Michael) (Entered: 07/17/2017)
07/18/2017		Minute Entry for proceedings held before Judge Nicholas G. Garaufis: Oral Argument re non−party Linode LLC's 82 motion to quash subpoena to testify. Counsel for Linode and the Government present. The court ORDERED the Government to file a revised subpoena on the docket and reserved decision on the motion pending review of the new subpoena. (Court Reporter Charleane Heading) (Houlihan, Michael) (Entered: 07/18/2017)
07/18/2017	118	Letter *to the Court Submitting a Revised Subpoena to Linode* as to Fabio Gasperini (Attachments: # 1 Exhibit Subpoena) (Komatireddy, Saritha) (Entered: 07/18/2017)
07/19/2017	120	Letter *summary of expert testimony* as to Fabio Gasperini (Bertollini, Simone) (Entered: 07/19/2017)

07/20/2017	121	MEMORANDUM & ORDER, The Government's 80 Motion in Limine as to Fabio Gasperini (1) is GRANTED. At trial, Defendant is precluded from (i) arguing that the Government forged the copies of documents it produced to Defendant in discovery, or (ii) calling Assistant United States Attorney Saritha Komatireddy as a witness. So Ordered by Judge Nicholas G. Garaufis on 7/19/2017. (Lee, Tiffeny) (Entered: 07/20/2017)
07/21/2017	122	Letter *regarding motion in limine* as to Fabio Gasperini (Attachments: # 1 Proposed Order) (Bertollini, Simone) (Entered: 07/21/2017)
07/21/2017	124	Letter *to the Court enclosing Proposed Order to Facilitate Defendant's Use of Laptop Computer at Trial* as to Fabio Gasperini (Attachments: # 1 Proposed Order) (Komatireddy, Saritha) (Entered: 07/21/2017)
07/21/2017	125	MANDATE of USCA (certified copy) as to Fabio Gasperini. Upon due consideration of Appellant Fabio Gasperini's appeal from an order of the District Court directing Gasperini's detention pending trial, it is hereby ORDERED that the order of the District Court is AFFIRMED. It is further ORDERED that the June 1, 2017 motion to expedite the appeal, which was withdrawn on June 12, 2017, is DENIED as moot. Issued as Mandate: 7/21/17. USCA #17−1561 (McGee, Mary Ann) (Entered: 07/21/2017)
07/21/2017	126	Letter *revised proposed order* as to Fabio Gasperini (Bertollini, Simone) (Entered: 07/21/2017)
07/21/2017	127	ORDER as to Fabio Gasperini that the Director of Metropolitan Detention Center allow Defendant to receive and maintain in his possession the following items: 3 (three) dressshirts, 1 (one) pair of pants, 1 (one) belt, 1 (one) pair of dress shoes. IT IS FURTHER ORDERED that the Director of the Metropolitan Detention Center allow Defendant to wear civilian clothes during trial. IT IS FURTHER ORDERED that the Director of the Metropolitan Detention Center allow Defendant to transport his discovery laptop to Court during trial. So Ordered by Judge Nicholas G. Garaufis on 7/21/2017. (Lee, Tiffeny) (Entered: 07/21/2017)
07/21/2017	128	MEMORANDUM & ORDER as to Fabio Gasperini (1), Defendant's motions in limine (65 , 105 , 111) are GRANTED IN PART and DENIED IN PART, with ruling on certain questions RESERVED until trial. So Ordered by Judge Nicholas G. Garaufis on 7/21/2017. (Lee, Tiffeny) (Entered: 07/21/2017)
07/22/2017	130	Fourth MOTION in Limine by Fabio Gasperini. (Bertollini, Simone) (Entered: 07/22/2017)
07/22/2017	131	Letter *to the Court in response to the Court's July 21, 2017 Order* as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 07/22/2017)
07/22/2017	132	Letter *enclosing supplemental exhibits and 3500 material* as to Fabio Gasperini (Wells, Melody) (Entered: 07/22/2017)
07/23/2017	133	Letter *from the government to defense counsel regarding out−of−town witnesses* as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 07/23/2017)
07/24/2017	134	Order re Defendant's 130 fourth motion in limine. The motion is DENIED without prejudice. Defendant may renew his objection to those documents at trial. No further motions in limine will be entertained prior to trial. So Ordered by Judge Nicholas G. Garaufis on 07/24/2017. (Houlihan, Michael) (Entered: 07/24/2017)
07/24/2017	135	ORDER as to Fabio Gasperini, that personnel at the Metropolitan Detention Center shall deliver to the United States Marshal an HP laptop computer in the possession of the defendant, FABIO GASPERINI, when the defendant is transported by the United States Marshal on July 24, 2017 for the start of his trial before this Court and retain custody of such laptop computer for delivery to the defendant's attorney, Simone Bertollini, Esq., who will retrieve it from the United States Marshal at the courthouse for use by the defendant in the courtroom throughout the trial. See Order for further and complete detail. So Ordered by Judge Nicholas G. Garaufis on 7/21/2017. (Lee, Tiffeny) (Entered: 07/24/2017)
07/24/2017	136	Minute Entry for proceedings held before Magistrate Judge Marilyn D. Go: Jury Selection held on 7/24/2017 as to Fabio Gasperini. Appearances: Simone Bertollini

		present with the Defendant Fabio Gasperini; AUSAs Saritha Komatireddy, Melody Wells and Special Agent William McKeen present. Italian interpreters Maria Galetta and Anna Maria Marra present. Case Called. Jurors' voir dire. The parties exercise their peremptory challenges. The jurors are selected but not sworn. The trial will commence before Judge Garaufis on 7/25/2017. (Court Reporters: Victoria Torres−Butler, Linda Marino, Charleane Heading) (Tape #9:17−6:31.) (Lee, Tiffeny) (Entered: 07/25/2017)
07/25/2017	157	Minute Entry for proceedings held before Judge Nicholas G. Garaufis: Jury Trial as to Fabio Gasperini held on 7/25/2017. Jury sworn. Preliminary jury instructions. Opening statements. Witnesses called. Trial continued to 7/26/2017. (Court Reporter Michele Lucchese) (Lee, Tiffeny) (Entered: 08/08/2017)
07/26/2017	158	Minute Entry for proceedings held before Judge Nicholas G. Garaufis: Jury Trial as to Fabio Gasperini held on 7/26/2017. Witnesses called. Trial continued to 7/27/2017. (Court Reporter Michele Lucchese) (Lee, Tiffeny) (Entered: 08/08/2017)
07/27/2017	137	ORDER as to Defendant Fabio Gasperini. Attached is Court Exhibit 1, the Draft Jury Charge. Ordered by Judge Nicholas G. Garaufis on 07/27/2017. (Houlihan, Michael) (Entered: 07/27/2017)
07/27/2017	138	ORDER as to Defendant Fabio Gasperini. Attached is Court Exhibit 2, the Draft Verdict Sheet. Ordered by Judge Nicholas G. Garaufis on 07/27/2017. (Houlihan, Michael) (Entered: 07/27/2017)
07/27/2017	159	Minute Entry for proceedings held before Judge Nicholas G. Garaufis: Jury Trial as to Fabio Gasperini held on 7/27/2017. Witnesses called. Trial continued to 7/28/2017. (Court Reporter Michele Lucchese) (Lee, Tiffeny) (Entered: 08/08/2017)
07/28/2017	140	Letter *to the Court regarding Jury Instructions* as to Fabio Gasperini (Bertollini, Simone) (Entered: 07/28/2017)
07/28/2017	160	Minute Entry for proceedings held before Judge Nicholas G. Garaufis: Jury Trial as to Fabio Gasperini held on 7/28/2017. Charge conference held. Defense counsel waives defendant's appearance. Trial continued to 7/31/2017. (Court Reporter Michele Lucchese) (Lee, Tiffeny) (Entered: 08/08/2017)
07/29/2017	141	Letter *from the government to defense counsel providing notice of intent to impeach by evidence of prior criminal convictions* as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 07/29/2017)
07/29/2017	142	Fifth MOTION in Limine *to Bar impeachment of Defendant's witness* by Fabio Gasperini. (Bertollini, Simone) (Entered: 07/29/2017)
07/29/2017	143	Letter *to the Court regarding Jury Instructions* as to Fabio Gasperini (Bertollini, Simone) (Entered: 07/29/2017)
07/30/2017	144	Letter *regarding jury charge* as to Fabio Gasperini (Wells, Melody) (Entered: 07/30/2017)
07/30/2017	145	RESPONSE in Opposition re 142 Fifth MOTION in Limine *to Bar impeachment of Defendant's witness and Request to Impeach Pursuant to Rules 608 and 609* (Komatireddy, Saritha) (Entered: 07/30/2017)
07/31/2017	146	Letter *to the Court regarding discovery* as to Fabio Gasperini (Bertollini, Simone) (Entered: 07/31/2017)
07/31/2017	147	Letter *regarding discovery* as to Fabio Gasperini (Wells, Melody) (Entered: 07/31/2017)
07/31/2017	148	ORDER as to Defendant Fabio Gasperini. Attached is Court Exhibit 3, Draft Two of the Jury Charge. Ordered by Judge Nicholas G. Garaufis on 07/31/2017. (Houlihan, Michael) (Entered: 07/31/2017)
07/31/2017	149	ORDER as to Defendant Fabio Gasperini. Attached is Court Exhibit 4, a redline version of Draft Two of the Jury Charge. Ordered by Judge Nicholas G. Garaufis on 07/31/2017. (Houlihan, Michael) (Entered: 07/31/2017)

07/31/2017	161	Minute Entry for proceedings held before Judge Nicholas G. Garaufis: Jury Trial as to Fabio Gasperini held on 7/31/2017. Juror #5 excused. The motion in limine is denied on the record. Witnesses called. Trial continues 8/1/2017. (Court Reporter Stacy Mace) (Lee, Tiffeny) (Entered: 08/08/2017)
08/01/2017	162	Minute Entry for proceedings held before Judge Nicholas G. Garaufis: Jury Trial as to Fabio Gasperini held on 8/1/2017. Witnesses called. Trial continued to 8/2/2017. (Court Reporter Stacy Mace) (Lee, Tiffeny) (Entered: 08/08/2017)
08/02/2017	150	ORDER as to Defendant Fabio Gasperini. Attached is Court Exhibit 5, the Final Jury Charge. Ordered by Judge Nicholas G. Garaufis on 08/02/2017. (Houlihan, Michael) (Entered: 08/02/2017)
08/02/2017	151	ORDER as to Defendant Fabio Gasperini. Attached is Court Exhibit 6, the Verdict Sheet. Ordered by Judge Nicholas G. Garaufis on 08/02/2017. (Houlihan, Michael) (Main Document 151 replaced on 8/3/2017) (Lee, Tiffeny). (Entered: 08/02/2017)
08/02/2017	163	Minute Entry for proceedings held before Judge Nicholas G. Garaufis: Jury Trial as to Fabio Gasperini held on 8/2/2017. Witness called. Government rests. Rule 29 Moti0n denied, but can be renewed after the defense case is made. Witness called. Defense rests. Rule 29 Motion denied. Summations. Trial continued to 8/3/2017. (Court Reporter Stacy Mace) (Lee, Tiffeny) (Entered: 08/08/2017)
08/03/2017	164	Minute Entry for proceedings held before Judge Nicholas G. Garaufis: Jury Trial as to Fabio Gasperini held on 8/3/2017. Charge of the Court. Marshal sworn. Jury deliberations. Trial continued to 8/4/2017. (Court Reporter Stacy Mace.) (Lee, Tiffeny) (Entered: 08/08/2017)
08/03/2017	165	Order of Sustenance as to Fabio Gasperini. So Ordered by Judge Nicholas G. Garaufis on 8/3/2017. (Lee, Tiffeny) (Entered: 08/08/2017)
08/04/2017	166	Minute Entry for proceedings held before Judge Nicholas G. Garaufis: Jury Trial as to Fabio Gasperini held on 8/4/2017. Jury deliberations. Verdict; See verdict sheet. Sentencing to lesser included charge is scheduled for 9/6/2017 at 01:00 PM in Courtroom 4D South before Judge Nicholas G. Garaufis. (Court Reporter Stacy Mace) (Lee, Tiffeny) (Entered: 08/08/2017)
08/04/2017	167	Order of Sustenance as to Fabio Gasperini. So Ordered by Judge Nicholas G. Garaufis on 8/4/2017. (Lee, Tiffeny) (Entered: 08/08/2017)
08/04/2017	168	JURY VERDICT as to Fabio Gasperini (1) Guilty of Lesser Offense Count 2; Fabio Gasperini (1) Not Guilty on Count 1,3,4,5. (Lee, Tiffeny) (Entered: 08/08/2017)
08/04/2017	169	Jury Notes (Court Exhibits 7−15) as to Fabio Gasperini. (Lee, Tiffeny) (Entered: 08/08/2017)
08/05/2017	152	MOTION for Release from Custody by Fabio Gasperini. (Attachments: # 1 Exhibit A, # 2 Exhibit B) (Bertollini, Simone) (Entered: 08/05/2017)
08/07/2017	153	REDACTION by USA to 1 Complaint as to Fabio Gasperini. (Lee, Tiffeny) (Entered: 08/07/2017)
08/07/2017	154	REDACTION by USA to 27 Memorandum in Opposition as to Fabio Gasperini. (Lee, Tiffeny) (Entered: 08/07/2017)
08/07/2017	155	REDACTION by USA to [59−1] Exhibit A to MOTION to Suppress *Evidence* as to Fabio Gasperini. (Lee, Tiffeny) (Entered: 08/07/2017)
08/08/2017	156	Letter *re sentencing* as to Fabio Gasperini (Wells, Melody) (Entered: 08/08/2017)
08/08/2017	170	NOTICE OF APPEAL from 176 Judgment entered 8/11/17 by Attorney for Fabio Gasperini. Filing fee $ 505, receipt number 0207−9742820. Service done electronically. (Bertollini, Simone) Modified on 8/11/2017 to reflect Judgment and Service. (McGee, Mary Ann). (Entered: 08/08/2017)
08/09/2017	171	SENTENCING MEMORANDUM by Fabio Gasperini (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit C) (Bertollini, Simone) (Entered: 08/09/2017)
08/09/2017	172	SENTENCING MEMORANDUM by USA as to Fabio Gasperini (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit C, # 4 Exhibit D) (Komatireddy, Saritha)

		(Entered: 08/09/2017)
08/09/2017	173	SENTENCING MEMORANDUM by USA as to Fabio Gasperini (Komatireddy, Saritha) (Entered: 08/09/2017)
08/09/2017	175	Minute Entry for proceedings held before Judge Nicholas G. Garaufis: Sentencing held on 8/9/2017 for Fabio Gasperini (1), Count(s) 1, 3, 4, 5, Found Not Guilty by Jury Verdict; Count(s) 2, Receives 12 months imprisonment; 1 year supervised release with special condition − compliance with Forfeiture Order to be filed within 90 days; $25.00 Assessment; $100,000 Fine. (Court Reporter Rivka Teich) (Lee, Tiffeny) (Entered: 08/11/2017)
08/10/2017	174	MOTION for Leave to Appeal In Forma Pauperis *for costs of trial transcripts* by Fabio Gasperini. (Attachments: # 1 Affidavit) (Bertollini, Simone) (Entered: 08/10/2017)
08/11/2017	176	JUDGMENT as to Fabio Gasperini (1), Count(s) 1, 3, 4, 5, Found Not Guilty by Jury Verdict; Count(s) 2, Receives 12 months imprisonment; 1 year supervised release with special condition − compliance with Forfeiture Order to be filed within 90 days; $25.00 Special Assessment; $100,000 Fine. So Ordered by Judge Nicholas G. Garaufis on 8/9/2017. (Attachments: # 1 Sentencing Transcript) (Lee, Tiffeny) (Entered: 08/11/2017)
08/11/2017		Electronic Index to Record on Appeal as to Fabio Gasperini sent to US Court of Appeals 170 Notice of Appeal − Final Judgment, Documents are available via Pacer. For docket entries without a hyperlink or for documents under seal, contact the court and we'll arrange for the document(s) to be made available to you. (McGee, Mary Ann) (Entered: 08/11/2017)
08/11/2017	178	MOTION to Amend/Correct 176 Judgment, by Fabio Gasperini. (Attachments: # 1 Exhibit, # 2 Exhibit) (Bertollini, Simone) (Entered: 08/11/2017)

AO 245B (Rev. 11/16) Judgment in a Criminal Case
Sheet 1

UNITED STATES DISTRICT COURT

Eastern District of New York

UNITED STATES OF AMERICA
v.
FABIO GASPERINI

JUDGMENT IN A CRIMINAL CASE

Case Number: CR 16-0441 (NGG)

USM Number: 90100-053

Simone Bertollini, Esq.
Defendant's Attorney

THE DEFENDANT:

X was found guilty by jury verdict on Count Two (2) of the Indictment.

☐ pleaded nolo contendere to count(s) _____ which was accepted by the court.

☐ was found guilty on count(s) _____ after a plea of not guilty.

The defendant is adjudicated guilty of these offenses:

Title & Section	Nature of Offense	Offense Ended	Count
18 U.S.C. § 1030(a)(2)	COMPUTER INTRUSION	June 2016	2

The defendant is sentenced as provided in pages 2 through 7 of this judgment. The sentence is imposed pursuant to the Sentencing Reform Act of 1984.

X The defendant was found not guilty by jury verdict on Counts 1, 3, 4 & 5 of the Indictment

☐ Count(s) _____ ☐ is ☐ are dismissed on the motion of the United States.

☐ Any underlying Indictment is dismissed on the motion of the United States.

It is ordered that the defendant must notify the United States attorney for this district within 30 days of any change of name, residence, or mailing address until all fines, restitution, costs, and special assessments imposed by this judgment are fully paid. If ordered to pay restitution, the defendant must notify the court and United States attorney of material changes in economic circumstances.

August 9, 2017
Date of Imposition of Judgment

s/Nicholas G. Garaufis
Signature of Judge

NICHOLAS G. GARAUFIS, U.S.D.J.
Name and Title of Judge

August 9, 2017
Date

DEFENDANT: FABIO GASPERINI
CASE NUMBER: CR 16-0441 (NGG)

IMPRISONMENT

The defendant is hereby committed to the custody of the Federal Bureau of Prisons to be imprisoned for a total term of: TWELVE (12) MONTHS (CAG) ON COUNT TWO (2) OF THE INDICTMENT.

☐ The court makes the following recommendations to the Bureau of Prisons:

X The defendant is remanded to the custody of the United States Marshal.

☐ The defendant shall surrender to the United States Marshal for this district:

☐ at _____ ☐ a.m. ☐ p.m. on _____ .

☐ as notified by the United States Marshal.

☐ The defendant shall surrender for service of sentence at the institution designated by the Bureau of Prisons:

☐ before 2 p.m. on _____ .

☐ as notified by the United States Marshal.

☐ as notified by the Probation or Pretrial Services Office.

RETURN

I have executed this judgment as follows:

Defendant delivered on _____ to _____

at _____ , with a certified copy of this judgment.

_____
UNITED STATES MARSHAL

By _____
DEPUTY UNITED STATES MARSHAL

DEFENDANT: FABIO GASPERINI
CASE NUMBER: CR 16-0441 (NGG)

SUPERVISED RELEASE

Upon release from imprisonment, you will be on supervised release for a term of : ONE (1) YEAR ON COUNT TWO (2) OF THE INDICTMENT.

MANDATORY CONDITIONS

1. You must not commit another federal, state or local crime.
2. You must not unlawfully possess a controlled substance.
3. You must refrain from any unlawful use of a controlled substance. You must submit to one drug test within 15 days of release from imprisonment and at least two periodic drug tests thereafter, as determined by the court.
   ☐ The above drug testing condition is suspended, based on the court's determination that you pose a low risk of future substance abuse. *(check if applicable)*
4. ☐ You must cooperate in the collection of DNA as directed by the probation officer. *(check if applicable)*
5. ☐ You must comply with the requirements of the Sex Offender Registration and Notification Act (42 U.S.C. § 16901, *et seq.*) as directed by the probation officer, the Bureau of Prisons, or any state sex offender registration agency in the location where you reside, work, are a student, or were convicted of a qualifying offense. *(check if applicable)*
6. ☐ You must participate in an approved program for domestic violence. *(check if applicable)*

You must comply with the standard conditions that have been adopted by this court as well as with any other conditions on the attached page.

DEFENDANT: FABIO GASPERINI
CASE NUMBER: CR 16-0441 (NGG)

STANDARD CONDITIONS OF SUPERVISION

As part of your supervised release, you must comply with the following standard conditions of supervision. These conditions are imposed because they establish the basic expectations for your behavior while on supervision and identify the minimum tools needed by probation officers to keep informed, report to the court about, and bring about improvements in your conduct and condition.

1. You must report to the probation office in the federal judicial district where you are authorized to reside within 72 hours of your release from imprisonment, unless the probation officer instructs you to report to a different probation office or within a different time frame.
2. After initially reporting to the probation office, you will receive instructions from the court or the probation officer about how and when you must report to the probation officer, and you must report to the probation officer as instructed.
3. You must not knowingly leave the federal judicial district where you are authorized to reside without first getting permission from the court or the probation officer.
4. You must answer truthfully the questions asked by your probation officer.
5. You must live at a place approved by the probation officer. If you plan to change where you live or anything about your living arrangements (such as the people you live with), you must notify the probation officer at least 10 days before the change. If notifying the probation officer in advance is not possible due to unanticipated circumstances, you must notify the probation officer within 72 hours of becoming aware of a change or expected change.
6. You must allow the probation officer to visit you at any time at your home or elsewhere, and you must permit the probation officer to take any items prohibited by the conditions of your supervision that he or she observes in plain view.
7. You must work full time (at least 30 hours per week) at a lawful type of employment, unless the probation officer excuses you from doing so. If you do not have full-time employment you must try to find full-time employment, unless the probation officer excuses you from doing so. If you plan to change where you work or anything about your work (such as your position or your job responsibilities), you must notify the probation officer at least 10 days before the change. If notifying the probation officer at least 10 days in advance is not possible due to unanticipated circumstances, you must notify the probation officer within 72 hours of becoming aware of a change or expected change.
8. You must not communicate or interact with someone you know is engaged in criminal activity. If you know someone has been convicted of a felony, you must not knowingly communicate or interact with that person without first getting the permission of the probation officer.
9. If you are arrested or questioned by a law enforcement officer, you must notify the probation officer within 72 hours.
10. You must not own, possess, or have access to a firearm, ammunition, destructive device, or dangerous weapon (i.e., anything that was designed, or was modified for, the specific purpose of causing bodily injury or death to another person such as nunchakus or tasers).
11. You must not act or make any agreement with a law enforcement agency to act as a confidential human source or informant without first getting the permission of the court.
12. If the probation officer determines that you pose a risk to another person (including an organization), the probation officer may require you to notify the person about the risk and you must comply with that instruction. The probation officer may contact the person and confirm that you have notified the person about the risk.
13. You must follow the instructions of the probation officer related to the conditions of supervision.

U.S. Probation Office Use Only

A U.S. probation officer has instructed me on the conditions specified by the court and has provided me with a written copy of this judgment containing these conditions. For further information regarding these conditions, see *Overview of Probation and Supervised Release Conditions*, available at: www.uscourts.gov.

Defendant's Signature _____ Date _____

DEFENDANT: FABIO GASPERINI
CASE NUMBER: CR 16-0441 (NGG)

SPECIAL CONDITIONS OF SUPERVISION

1. THE DEFENDANT SHALL COMPLY WITH THE ORDER OF FORFEITURE WHICH SHALL BE FILED WITHIN 90 DAYS.

DEFENDANT: FABIO GASPERINI
CASE NUMBER: CR 16-0441 (NGG)

CRIMINAL MONETARY PENALTIES

The defendant must pay the total criminal monetary penalties under the schedule of payments on Sheet 6.

	Assessment	JVTA Assessment*	Fine	Restitution
TOTALS	$ 25.00	$ N/A	$ 100,000.00	$ N/A

☐ The determination of restitution is deferred until _____. An *Amended Judgment in a Criminal Case (AO 245C)* will be entered after such determination.

☐ The defendant must make restitution (including community restitution) to the following payees in the amount listed below.

If the defendant makes a partial payment, each payee shall receive an approximately proportioned payment, unless specified otherwise in the priority order or percentage payment column below. However, pursuant to 18 U.S.C. § 3664(i), all nonfederal victims must be paid before the United States is paid.

Name of Payee	Total Loss**	Restitution Ordered	Priority or Percentage

TOTALS $ _____ $ _____

☐ Restitution amount ordered pursuant to plea agreement $ _____

☐ The defendant must pay interest on restitution and a fine of more than $2,500, unless the restitution or fine is paid in full before the fifteenth day after the date of the judgment, pursuant to 18 U.S.C. § 3612(f). All of the payment options on Sheet 6 may be subject to penalties for delinquency and default, pursuant to 18 U.S.C. § 3612(g).

☐ The court determined that the defendant does not have the ability to pay interest and it is ordered that:

☐ the interest requirement is waived for the ☐ fine ☐ restitution.

☐ the interest requirement for the ☐ fine ☐ restitution is modified as follows:

* Justice for Victims of Trafficking Act of 2015, Pub. L. No. 114-22.
** Findings for the total amount of losses are required under Chapters 109A, 110, 110A, and 113A of Title 18 for offenses committed on or after September 13, 1994, but before April 23, 1996.

DEFENDANT: FABIO GASPERINI
CASE NUMBER: CR 16-0441 (NGG)

SCHEDULE OF PAYMENTS

Having assessed the defendant's ability to pay, payment of the total criminal monetary penalties is due as follows:

A X Special Assessment of $ 25.00 due immediately, balance due

☐ not later than ______________, or
☐ in accordance with ☐ C, ☐ D, ☐ E, or ☐ F below; or

B ☐ Payment to begin immediately (may be combined with ☐ C, ☐ D, or ☐ F below); or

C ☐ Payment in equal ________ *(e.g., weekly, monthly, quarterly)* installments of $ ________ over a period of ________ *(e.g., months or years)*, to commence ________ *(e.g., 30 or 60 days)* after the date of this judgment; or

D ☐ Payment in equal ________ *(e.g., weekly, monthly, quarterly)* installments of $ ________ over a period of ________ *(e.g., months or years)*, to commence ________ *(e.g., 30 or 60 days)* after release from imprisonment to a term of supervision; or

E ☐ Payment during the term of supervised release will commence within ________ *(e.g., 30 or 60 days)* after release from imprisonment. The court will set the payment plan based on an assessment of the defendant's ability to pay at that time; or

F X $100,000.00 fine payment due immediately.

Unless the court has expressly ordered otherwise, if this judgment imposes imprisonment, payment of criminal monetary penalties is due during the period of imprisonment. All criminal monetary penalties, except those payments made through the Federal Bureau of Prisons' Inmate Financial Responsibility Program, are made to the clerk of the court.

The defendant shall receive credit for all payments previously made toward any criminal monetary penalties imposed.

☐ Joint and Several

Defendant and Co-Defendant Names and Case Numbers *(including defendant number)*, Total Amount, Joint and Several Amount, and corresponding payee, if appropriate.

☐ The defendant shall pay the cost of prosecution.

☐ The defendant shall pay the following court cost(s):

☐ The defendant shall forfeit the defendant's interest in the following property to the United States:

Payments shall be applied in the following order: (1) assessment, (2) restitution principal, (3) restitution interest, (4) fine principal, (5) fine interest, (6) community restitution, (7) JVTA assessment, (8) penalties, and (9) costs, including cost of prosecution and court costs.

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X
UNITED STATES OF AMERICA,

-against-

FABIO GASPERINI

Defendant.
----------X

VERDICT SHEET

16-CR-441 (NGG)

COUNT ONE
(Computer Intrusion in Furtherance of Fraud, 18 U.S.C § 1030(a)(4))

1. As to Count One, do you find the defendant:

Guilty_____ Not Guilty✓_____

COUNT TWO
(Computer Intrusion and Obtaining Information, 18 U.S.C §§ 1030(a)(2), 1030(c)(2)(B),)

2. As to Count Two, do you find the defendant:

Guilty_____ Not Guilty✓_____

If your answer to Question 2 is not guilty, proceed to question 2(a). If your answer is guilty, proceed to Question 3.

2a. As to the lesser included offense in Count Two, do you find the defendant:

Guilty✓_____ Not Guilty_____

Proceed to Question 3

COUNT THREE
(Wire Fraud Conspiracy, 18 U.S.C. § 1349)

3. As to Count Three, do you find the defendant:

Guilty_____ Not Guilty ✓

COUNT FOUR
(Wire Fraud, 18 U.S.C. § 1343)

4. As to Count Four, do you find the defendant:

Guilty_____ Not Guilty ✓

COUNT FIVE
(Money Laundering Conspiracy 18 U.S.C. § 1956(h))

1. As to Count Five, do you find the defendant:

Guilty_____ Not Guilty ✓

Dated: Brooklyn, New York
August 4, 2017

William F. Branco
Jury Foreperson

Your deliberations are complete. Advise the Court by note that you have reached a verdict.

MR. BERTOLLINI: No, your Honor.

THE COURT: All right. With regard to the computation of the guideline, the Court agrees that the jury determined as to Counts One, Three, Four, Five that the Government had not met its burden of prove beyond a reasonable doubt. But the Court also concludes based on the evidence that was presented during the course of the trial that it has more than met its obligation of proving by a preponderance of the evidence that all of the factors that were articulated by the Government in its statement now have been met. In fact, there is substantial documentary and testimonial evidence of the existence of the botnet, of the fraudulent scheme, and of the injury that occurred to individuals, to entities, to Government agencies, and that the defendant engaged in obstruction of justice. And therefore, the Court agrees with the Government that all of the enhancements that are set forth on page five of the Government's submission have been proven by a preponderance of the evidence.

Therefore, the defense's objections are overruled and the Court finds the total offense level is 26, defendant is a criminal history I, the range of imprisonment is 63 to 78 months of imprisonment under the guideline. But the effective guideline is 12 months because there is a statutory maximum sentence of 12 months for the lesser included offense of Count Two. So that takes care of the guideline calculation, and

defense has its exception.

The next step is to consider the factors under section 3553(a) of Title 18 of the United States Code to establish a sentence that is sufficient but not greater than that necessary to fulfill the purposes of sentencing, and so on that I will hear from the Government first. Is there anything more that you want to say?

MS. KOMATIREDDY: Your Honor, nothing to add.

THE COURT: All right. Let me hear from the defense, is there more that you have to say?

MR. BERTOLLINI: No, your Honor, thank you.

THE COURT: Is there anything that the defendant would like to say before I sentence him on the lesser included offense of Count Two?

THE DEFENDANT: No, your Honor.

THE COURT: The $100 special assessment is not $100 in this case, is it?

MS. KOMATIREDDY: I think it's $25, your Honor.

THE COURT: It is $25.

Please rise. Mr. Gasperini, I sentence you as follows: Twelve months in the custody of the Attorney General and a maximum fine of $100,000, a one-year term of supervised release, forfeiture of your the botnet that was identified during the course of the trial, the infrastructure used to manage and run the botnet, the computers many command and

control servers, and domains and Mr. Gasperini's backdoor with username request. There is a $25 special assessment, which is mandatory.

You have the right to appeal your sentence to the United States Court of Appeals for the Second Circuit if you believe the Court has not properly followed the law in sentencing you. Your time to appeal is extremely limited. You should discuss with your attorney whether an appeal would be worthwhile.

You are also subject to removal from the United States at the conclusion of your prison sentence in a separate proceeding brought by the Department of Homeland Security.

I'm going give the Government 90 days to provide additional forfeiture information in connection with these rather technical items of forfeiture. I'm not imposing a restitution requirement because of the difficulty of providing restitution.

Is there anything further from the Government for today?

MS. KOMATIREDDY: No, your Honor.

THE COURT: Anything from the defense?

MR. BERTOLLINI: No, your Honor.

THE COURT: All right, we're adjourned.

CR 16 - 441

RMT:SK
F. #2015R00439

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

GARAUFIS, J.

– – – – – – – – – – – – – – – – X

UNITED STATES OF AMERICA

- against -

FABIO GASPERINI,

Defendant.

INDICTMENT

REYES, M.J.

Cr. No. _____

(T. 18, U.S.C., §§ 981(a)(1)(C), 982(a)(1), 982(a)(2)(B), 1030(a)(2), 1030(a)(4), 1030(b), 1030(c)(2)(A), 1030(c)(2)(B), 1030(c)(3)(A), 1030(i), 1343, 1349, 1956(h), 2 and 3551 et seq.; T. 21, U.S.C., § 853(p); T. 28, U.S.C., § 2461(c))

– – – – – – – – – – – – – – – – X

THE GRAND JURY CHARGES:

INTRODUCTION

At all times relevant to this Indictment, unless otherwise indicated:

Botnets and Click Fraud

1. A botnet is a network of computers (such as servers) infected with malicious software without the users' knowledge or authorization. A malicious actor can remotely control the computers (which are described individually as "bots") and draw upon the bandwidth and computing power of the individual bots for many malicious purposes, including to launch denial-of-service attacks, deliver large-scale spam campaigns, transmit viruses or spyware, steal banking credentials or personally identifiable information, perform far-reaching vulnerability scans, perpetrate click fraud, and engage in other acts of cybercrime.

2. In general, "click fraud" is a type of cybercrime in which a malicious actor fraudulently obtains money from advertising companies and businesses.

3. Businesses commonly hire online advertising companies to send traffic to their websites. These advertising companies in turn contract with individuals, typically someone who operates a website, to place on the website certain links advertising the businesses' products or services, and are then compensated based upon the number of visitors to the website that click on the link. The advertising companies typically pay the individuals on a per-click basis.

4. To conduct a click fraud scheme, a malicious actor can, for example, remotely command a botnet to flood a particular website advertisement with electronic communications that register with the advertising company as clicks by a human user on the advertisement. This type of command falsely and fraudulently inflates the number of clicks reported to the advertising companies, causing them to pay for clicks perpetrated by automated bots rather than clicks completed by potential customers who, in fact, viewed and clicked on the advertisements.

The Defendant and the Fraudulent Scheme

5. The defendant FABIO GASPERINI was an information technology professional in Rome, Italy.

6. In or about and between February 2011 and June 2016, the defendant FABIO GASPERINI, together with others, surreptitiously gained entry into multiple computer servers (the "compromised servers") in the United States and elsewhere that he did not have permission to access. The compromised servers included computer servers typically used for

large-scale data storage and transfer and that could serve various functions including as file servers, cloud-based servers and file transfer protocol servers.

7. It was a part of the scheme that the defendant FABIO GASPERINI, together with others, accessed the compromised servers without permission and installed on them malicious software that gave him remote access to, and control of, these compromised servers, which together constituted a botnet. In establishing this botnet, GASPERINI also obtained unauthorized access to sensitive data and files stored on the compromised servers.

8. It was further part of the scheme that the defendant FABIO GASPERINI, together with others, leased computer servers in the United States and elsewhere to manage the botnet. GASPERINI, together with others, used these leased servers to provide instructions and resources to the compromised servers in the botnet.

9. It was further part of the scheme that the defendant FABIO GASPERINI, together with others, used the botnet to perpetrate, among other things, click fraud. GASPERINI installed on the compromised servers malicious computer scripts that were designed to cause the compromised servers to execute specific commands, and then caused the compromised servers to effect automated clicks on advertisements appearing on particular websites. In doing so, GASPERINI fraudulently generated revenue from advertising companies and businesses.

10. It was further part of the scheme that the defendant FABIO GASPERINI, together with others, sent and received some of the payments related to click fraud through other individuals in order to conceal the nature of the payments and his identity.

COUNT ONE
(Computer Intrusion)

11. The allegations contained in paragraphs one through ten are realleged and incorporated as though fully set forth in this paragraph.

12. In or about and between February 2011 and June 2016, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant FABIO GASPERINI, together with others, did knowingly and with intent to defraud access, and attempt to access, one or more protected computers without authorization, and exceed authorized access, and by means of such conduct did further the intended fraud and obtain something of value, to wit: the use of a computer, information, and United States and foreign currency.

(Title 18, United States Code, Sections 1030(a)(4), 1030(b), 1030(c)(3)(A), 2 and 3551 et seq.)

COUNT TWO
(Computer Intrusion)

13. The allegations contained in paragraphs one through ten are realleged and incorporated as though fully set forth in this paragraph.

14. In or about and between February 2011 and June 2016, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant FABIO GASPERINI, together with others, did knowingly and intentionally access, and attempt to access, one or more computers without authorization and exceed authorized access, and thereby did obtain information from one or more protected computers for the purpose of commercial advantage and private financial gain, and in furtherance of criminal

and tortious acts in violation of the laws of the United States and any State, and the value of the information obtained exceeded $5,000.

(Title 18, United States Code, Sections 1030(a)(2), 1030(b), 1030(c)(2)(A), 1030(c)(2)(B), 2 and 3551 et seq.)

COUNT THREE
(Wire Fraud Conspiracy)

15. The allegations contained in paragraphs one through ten are realleged and incorporated as though fully set forth in this paragraph.

16. In or about and between February 2011 and June 2016, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant FABIO GASPERINI, together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud advertising companies and businesses, and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, to wit: remote access of computers and servers in the United States and elsewhere, online payments, credit and debit card transactions, and emails, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNT FOUR
(Wire Fraud)

17. The allegations contained in paragraphs one through ten are realleged and incorporated as though fully set forth in this paragraph.

18. In or about and between February 2011 and June 2016, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant FABIO GASPERINI, together with others, did knowingly and intentionally devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises.

19. On December 8, 2014, for the purpose of executing such scheme and artifice, and attempting to do so, the defendant FABIO GASPERINI did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures and sounds, to wit: a request from a compromised server located in Queens, New York, to a server located outside of New York State, for the transfer of a user agent string.

(Title 18, United States Code, Sections 1343, 2 and 3551 et seq.)

COUNT FIVE
(Money Laundering Conspiracy)

20. The allegations contained in paragraphs one through ten are realleged and incorporated as though fully set forth in this paragraph.

21. In or about and between February 2011 and June 2016, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant FABIO GASPERINI, together with others, did knowingly and intentionally

conspire to conduct one or more financial transactions in and affecting interstate and foreign commerce, which transactions in fact involved the proceeds of specified unlawful activity, to wit: computer intrusion, wire fraud and wire fraud conspiracy, in violation of Title 18, United States Code, Sections 1030(a)(2), 1030(a)(4), 1343 and 1349, knowing that the property involved in the transactions represented the proceeds of some form of unlawful activity, and knowing that the transactions were designed in whole and in part to conceal and disguise the nature, the location, the source, the ownership and the control of the proceeds of the specified unlawful activity, contrary to Title 18, United States Code, Section 1956(a)(1)(B)(i).

(Title 18, United States Code, Sections 1956(h) and 3551 et seq.)

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNTS ONE AND TWO

22. The United States hereby gives notice to the defendant that, upon his conviction of either of the offenses charged in Counts One and Two, the government will seek forfeiture in accordance with Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), which require the forfeiture of such person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation, and any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

23. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

(a) cannot be located upon the exercise of due diligence;

(b) has been transferred or sold to, or deposited with, a third party;

(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 cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendant up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i); Title 21, United States Code, Section 853(p))

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNTS THREE AND FOUR

24. The United States hereby gives notice to the defendant that, upon his conviction of either offense charged in Counts Three and Four, the government will seek forfeiture in accordance with Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), which require any person convicted of such offenses to forfeit any property, real or personal, which constitutes or is derived from proceeds traceable to violations of Title 18, United States Code, Sections 1349 and 1343.

25. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

(a) cannot be located upon the exercise of due diligence;

(b) has been transferred or sold to, or deposited with, a third party;

(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 cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendant up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Section 981(a)(1)(C); Title 21, United States Code, Section 853(p); Title 28, United States Code, Section 2461(c))

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNT FIVE

26. The United States hereby gives notice to the defendant that, upon his conviction of the offense charged in Count Five, the government will seek forfeiture in accordance with Title 18, United States Code, Section 982(a)(1), which requires any person convicted of such offense to forfeit any property, real or personal, involved in such offense, or any property traceable to such property.

27. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

(a) cannot be located upon the exercise of due diligence;

(b) has been transferred or sold to, or deposited with, a third party;

(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 cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendant up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Section 982(a)(1); Title 21, United States Code, Section 853(p))

A TRUE BILL

FOREPERSON

ROBERT L. CAPERS
UNITED STATES ATTORNEY
EASTERN DISTRICT OF NEW YORK

BY: _____
ACTING UNITED STATES ATTORNEY
PURSUANT TO 28 C.F.R. 0.136

U.S. Department of Justice

United States Attorney
Eastern District of New York

271 Cadman Plaza East
Brooklyn, New York 11201

MW/SK
F. #2015R00439

June 9, 2017

By Hand and ECF

The Hon. Nicholas G. Garaufis
United States District Judge
Eastern District of New York
225 Cadman Plaza East
Brooklyn, New York 11201

Re: United States v. Fabio Gasperini
Criminal Docket No. 16-441 (NGG)

Dear Judge Garaufis:

Pursuant to the Court's June 1, 2017 Order granting in part and denying in part defendant Fabio Gasperini's motion for a bill of particulars ("Order"), the government lists below "the categories of information allegedly obtained in connection with the Computer Intrusion Counts." (Order, D.E. No. 45 at 19.) In accordance with the Order, identified below are the categories of information the government alleges the defendant obtained in connection with Counts One and Two of the Indictment:

1. Information Obtained from Port Scanning: During the relevant time period, the defendant obtained information from port scanning programs about computers on the internet, including: the IP addresses of scanned computers, the date and time period during which the scans were conducted, whether specified "ports"[1] were in use or available on the scanned computers, whether specified ports were accessible via

[1] A port provides a means of connection between computers for networking purposes. Ports can be physical (e.g., a connection for an Ethernet cable or other hardware) or logical. In computer networking, logical ports, or logical connection endpoints, allow software connections between software applications and programs. Logical ports are numbered 0 to 65535 and are identified by their assigned number. The ports described by the government here are logical ports.

remote connection, and whether the scanned computers had certain vulnerabilities or were vulnerable to certain exploits, such as a Shellshock exploit.

2. Information Obtained When the Defendant's Malware Infected Computers: As alleged in the Indictment, the defendant accessed computers without permission and installed on them malicious software that gave him remote access to, and control of, those computers (the "compromised servers"). The defendant installed on the compromised servers malicious computer scripts that were designed to cause the compromised servers to execute specific commands, and then caused the compromised servers to effect automated clicks on advertisements appearing on websites that the defendant owned and operated. In the process of installing this malicious software, the defendant obtained information about the existing settings of the compromised servers. For example, he obtained information about whether specified ports and usernames were available for use, and if he determined that they were available for use, manipulated the settings of the compromised servers. The defendant also installed port scanning programs onto the compromised servers and thereby obtained information about other computers and servers on the internet, as described above. He also patched, or closed, the vulnerability that allowed his malware to infect the compromised servers, making it impossible for others to access the server through the same vulnerability. However, the defendant also created a new user account, i.e., a backdoor, that allowed him to continue to login to the compromised servers at will, and evidence at trial will show that he used that backdoor access on multiple occasions. As a result, the defendant obtained information including the contents of the compromised servers, which included sensitive information including financial and payment records, personally identifying information, credit card information, and tax records.

3. Information Obtained from Computers that the Defendant Leased and Used: As alleged in the Indictment, the defendant leased computers (the "leased servers") to manage the botnet and used those leased servers to provide instructions and resources to the compromised servers in the botnet. Some of the leased servers functioned as IRC servers and web servers. The defendant obtained information from the leased servers on a regular basis, including files he stored on the leased servers, the results of scanning activity, password-cracking activity, Metasploit activity, and other malicious activity conducted through the leased servers, and logs related to the activities of scanned computers and connecting computers (see infra). The defendant also used the compromised servers to obtain information from the leased servers, including malicious computer scripts, user agent strings, Lightaidra and IRC files, and scanning and configuration files.

4. Information Obtained from the Connecting Computers: During the relevant time period, the defendant obtained information from the compromised servers and other computers (collectively, the "connecting computers") that connected to the defendant's computers and leased servers including: the IP address of the connecting computers, the date and time of the connection, the "request" or message from the connecting computers, the status of the request (e.g., whether the request was successful, whether connections have been closed, whether there was an error or whether the computer was still trying to connect), the size of the request from the connecting computers, the website or location that referred the connecting computers to the defendant's computers and leased servers, the user agent associated with the connecting computers (i.e., the software agent used to connect, commonly a web browser such as Mozilla), instances in which the connecting computers were using the user agent string employed by the defendant in connection with his click fraud scheme, instances in which the connecting computers clicked on an advertisement hosted on a website, password and shadow files from connecting computers, and user data and content from connecting computers.

The government reserves the right to amend this bill of particulars. See Fed. R. Crim. P. 7(f) ("The government may amend a bill of particulars subject to such conditions as justice requires."); United States v. Salazar, 485 F.2d 1272, 1277 (2d Cir. 1973) (affirming district court's acceptance of supplemental bill of particulars).

Respectfully submitted,

BRIDGET M. ROHDE
Acting United States Attorney

By: /s/
Saritha Komatireddy
Melody Wells
Assistant U.S. Attorneys
(718) 254-7000

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

UNITED STATES OF AMERICA

-against-

FABIO GASPERINI,

Defendant.

MEMORANDUM & ORDER

16-CR-441 (NGG)

----------X

NICHOLAS G. GARAUFIS, United States District Judge.

Defendant Fabio Gasperini ("Defendant") is charged with two counts of computer intrusion, one count of conspiracy to commit wire fraud, one count of wire fraud, and one count of conspiracy to commit money laundering. (See Indictment ("Ind.") (Dkt. 3) ¶¶ 11-21.) The charges stem from Defendant's alleged creation of a "botnet" to further a "click fraud" perpetrated against advertising companies. (Id. ¶¶ 1-10.) The Government alleges that Defendant and others obtained unauthorized access to computers in the U.S. and around the world and remotely directed those computers to fraudulently inflate the number of times that online advertisements were "viewed."

Currently pending before the court are Defendant's motion to dismiss the indictment (Mot. to Dismiss ("MTD") (Dkt. 9)), motion for a bill of particulars (Mot. for Bill of Particulars ("BOP Mot.") (Dkt. 36)), and motion for disclosure of grand jury materials (Mot. for Grand Jury Tr. ("GJ Mot.") (Dkt. 35)). For the following reasons, Defendant's motions to dismiss and for disclosure of grand jury materials are DENIED and his motion for a bill of particulars is GRANTED IN PART and DENIED IN PART.

I. BACKGROUND

A. Allegations

The following statement of facts is drawn from the Indictment, the Complaint, and an Affidavit submitted in connection with Defendant's extradition to the United States.

Defendant is an Italian national who resided in Rome at all relevant times. (Ind. ¶ 1.) The Government's primary allegation is that Defendant engaged in "click fraud," a scheme in which an individual:

1) enters into a contract with an advertising company in which the individual (a) places online advertisements onto a websites and (b) receives compensation from the company based on the number of times that users "click" on their ads, and then

2) places malicious software ("malware") onto one or more third-party computers and servers that directs those computers to click on their advertisements and artificially drives up the number of "clicks" for which the individual is compensated.

(See id. ¶¶ 1-4.) In connection with these schemes, individuals may develop a "botnet," defined by the Indictment as "a network of computers, such as servers, infected with malicious software without the users' knowledge or authorization." (Id. ¶ 1.) The botnet's creator can then remotely direct the network of compromised computers to engage in coordinated action and, in a "click fraud" scheme, can "remotely command a botnet to flood a particular website advertisement with electronic communications that register with the advertising company as clicks by a human user." (Id. ¶ 4.)

The Indictment alleges that between February 2011 and June 2016, Defendant and others "surreptitiously gained entry into multiple computer servers . . . in the United States and elsewhere" without authorization (id. ¶ 6) and "installed . . . malicious software," creating a

botnet (id. ¶ 7). The Indictment alleges that, "[i]n establishing this botnet, [Defendant] also obtained unauthorized access to sensitive data and files stored on the compromised servers." (Id.) Defendant allegedly used the botnet to commit "click fraud" against various businesses and advertising companies, including one named Italian advertising company. (Ex. A. to Opp'n to MTD ("Extradition Aff.") (Dkt. 27-1) ¶ 10.) The Indictment further alleges that Defendant laundered proceeds from the alleged "click fraud" through other individuals "in order to conceal the nature of the payments and his identity." (Ind.¶ 10.)

B. Procedural History

Defendant was arrested in Amsterdam in June 18, 2016, and extradited to the United States on April 20, 2017. (Opp'n to MTD ("MTD Opp'n") (Dkt. 27) at 2.) On August 4, 2016, a federal grand jury returned an Indictment charging Defendant with two counts of computer intrusion (the "Computer Intrusion Counts"), wire fraud and conspiracy to commit wire fraud (the "Wire Fraud Counts"); and conspiracy to launder money. (Ind. ¶¶ 11-21.)

On April 24, 2017, Defendant moved to dismiss the Indictment. (See MTD). Defendant subsequently moved for both a bill of particulars and for disclosure of grand jury material. (See BOP Mot.; GJ Mot.)

II. DISCUSSION

A. Motion to Dismiss the Indictment

Defendant's motion to dismiss asserts three primary arguments: (1) the Computer Intrusion Counts under 18 U.S.C. §§ 1030(a)(2) and 1034(a)(4) are insufficiently pled; (2) the statutes underlying the Wire Fraud Counts cannot be applied extraterritorially; and (3) application of the Wire Fraud and Computer Intrusion Counts to Defendant would violate his due process rights. (MTD at 2.) The court disagrees with Defendant on each of these points and accordingly denies Defendant's motion to dismiss.

1. Legal Standard

"[An] indictment . . . must be a plain, concise, and definite written statement of the essential facts constituting the offense charged . . . ." Fed. R. Crim. P. 7(c). "[A]n indictment is sufficient if it, first, contains the elements of the offense charged and fairly informs a defendant of the charge against which he must defend, and, second, enables him to plead an acquittal or convictions in bar of future prosecutions for the same offense." United States v. Alfonso, 143 F.3d 772, 776 (2d Cir. 1998) (quoting Hamling v. United States, 418 U.S. 87, 117 (1974)). This generally requires an Indictment to "do little more than [] track the language of the statute charged and state the place and time (in approximate terms) of the alleged crime." United States v. Walsh, 194 F.3d 37, 44 (2d Cir. 1999) (internal quotation marks and citations omitted).

Defendants may raise pretrial challenges to the sufficiency and specificity of an indictment "if the basis for the motion is reasonably available and the motion can be determined without a trial on the merits." See Fed. R. Crim. P. 12(b)(3)(B)(iii), (v). "[I]n deciding a pretrial motion to dismiss, the Court must accept the Government's factual allegations as true," United States v. Carnesi, 461 F. Supp. 2d 97, 98 (E.D.N.Y. 2006), and the "indictment must be read to include facts which are necessarily implied by the specific allegations made," United States v. Stavroulakis, 952 F.2d 686, 693 (2d Cir. 1992) (internal quotation marks and citation omitted).

2. Alleged Insufficiency of the Computer Intrusion Statutes

Defendant contends that the Indictment fails to allege several essential elements necessary to the Computer Intrusion Counts.[1] Specifically, Defendant argues that the Indictment fails to allege (1) that he accessed a "protected computer"; (2) that he gained "actual access" to

[1] Defendant's motion also states in passing that the Government fails to allege a prima facie case of wire fraud. (MTD at 3.) However, Defendant does not direct any of his arguments at the wire fraud charges, and the basis for his claim is unclear from the face of the Indictment. The court finds no reason to conclude that the Wire Fraud Counts are insufficiently pled and does not further address the point in this opinion.

information on those computers; (3) that he "obtained information" through the alleged unauthorized access; and (4) that Defendant derived any value from the intrusions. (See generally MTD at 3-6.) Before addressing these alleged insufficiencies, the court briefly reviews the statutes at issue in those counts and identifies the elements that the Government must allege in the Indictment. The court concludes that the Indictment contains sufficient allegations to survive a motion to dismiss.

a. The Computer Intrusion Statutes

i. 18 U.S.C. § 1030(a)(4) (Count One)

Section 1030(a)(4) states that:

> [Whoever] knowingly and with intent to defraud, accesses a protected computer without authorization . . . and by means of such conduct furthers the intended fraud and obtains anything of value [commits a crime], unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.

18 U.S.C. § 1030(a)(4) (emphasis added). A "protected computer" is, inter alia, "a computer [] which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication." Id. § 1030(e)(2)(B). Courts have interpreted this definition to include "effectively all computers with Internet access." United States v. Valle, 807 F.3d 508, 528 (2d Cir. 2015) (quoting United States v. Nosal, 676 F.3d 854, 859 (9th Cir. 2012)).

ii. 18 U.S.C § 1030(a)(2) (Count Two)

Section 1030(a)(2) makes it a crime to "intentionally access[] a computer without authorization . . . and thereby obtain . . . [i]nformation from any protected computer." 18 U.S.C. § 1030(a)(2). "Protected computer" here has the same meaning as that noted above.

b. Alleged Defects

i. Failure to Allege Access to a Protected Computer

Defendant claims that the Indictment fails to sufficiently allege that he accessed a "protected computer." (See MTD at 4-5.) As noted, however, the term "protected computer" encompasses "effectively all computers with Internet access."[2] Valle, 807 F.3d at 528 (internal quotation marks and citation omitted). The allegations that Defendant transmitted malware electronically in support of an online click fraud scheme necessarily involve internet-connected computers. (See Ind. ¶ 5-10.) Moreover, the Indictment's recitation of both Computer Intrusion Counts alleges that he accessed "one or more protected computers." (Id. ¶¶ 12, 14) Both separately and taken together, these allegations are sufficient to inform the Defendant of the charge against him with respect to that element. See Stavroulakis, 952 F.2d at 693 (stating that the "indictment must be read to include facts which are necessarily implied by the specific allegations made.")

Accordingly, the court denies Defendant's motion to dismiss based on the claimed failure to allege that he accessed a "protected computer."

ii. Failure to Allege "Actual" Access

Defendant maintains that the Indictment fails to allege that he had "actual access" to any U.S. servers, and at most alleges control of an automated botnet that provided the "capability to intrude into computers." (MTD at 3.) In connection with this argument, Defendant points to a statement in the affidavit submitted in support of his extradition that Defendant's "malicious

[2] At oral argument, Defendant argued that the term "protected computer" had been read overly broadly, pointing to the other, more specific prohibitions in Section 1030(a)(2) that apply to information obtained from financial institutions, credit card issuers, and federal agencies and departments. (Tr. of Hr'g on Mots. ("Hr'g Tr.") (Docket Number forthcoming) at 7-8.) However, given the breadth of the statutory language and other cases interpreting that language, the court sees no reason to adopt a different interpretation of "protected computer" than that provided above, nor does Defendant provide a suggested alternative definition.

software was found" in Queens-based law firm's server. (Id. at 4 (citing Extradition Aff. ¶ 9).) Defendant claims this allegation cannot support actual access because, at the time the malware was "found," Defendant was in custody. (See MTD at 4.)

Despite Defendant's contentions, however, the Indictment avers at several points that Defendant had actual access to computer servers, including access gained as part of the process of installing the malware. (See Ind. ¶¶ 6, 7, 12, 13.) These statements track the language of the statute and, combined with the approximate statements of dates and locations contained in the Indictment, are sufficient to withstand a motion to dismiss at this stage.

To the extent that Defendant's challenge is based on the Extradition Affidavit, that argument is not properly raised in a motion to dismiss. In weighing the validity of the Indictment, the court may not consider outside evidence. See, e.g., United States v. Foxworth, No. 3:06-CR-81 (AHN), 2006 WL 3462657, at *3 (D. Conn. Nov. 16, 2006); cf. also United States v. Brown, 321 F. Supp. 2d 598, 600 (S.D.N.Y. 2004) ("[I]t is axiomatic that . . . a defendant may not challenge a facially valid indictment prior to trial for insufficient evidence."). Further, it is not clear that the affidavit in fact supports Defendant's position, as it alleges that Defendant "gained entry into multiple servers." (Extradition Aff. ¶ 5.)

For these reasons, the court denies Defendant's motion to dismiss based on the claimed failure to allege "actual access" to computer systems.

iii. Failure to Allege that Defendant "Obtained Information" From a Protected Computer

Defendant argues that Count Two is insufficiently pled because the alleged scheme did not target "information" on protected computers. (See, e.g., Def. Reply Mem. ("Reply") (Dkt. 30) at 2-3.) Pointing to Section 1030(a)(2)'s requirement that a defendant obtain information from a protected computer though their unauthorized access, 18 U.S.C. § 1030(a)(2),

Defendant argues that "criminal liability is triggered . . . [only based on] actual obtainment of information that is itself needed—and not collateral—to carry out the fraudulent scheme" (Reply at 2). From this, he claims that the Indictment fails as a matter of law because the purpose of the alleged intrusion "was not the information that [the compromised computers] may or may not have contained, but rather the[ir] computing power." (Reply at 3.)

Whatever its merits, Defendant's argument is better considered at trial. The Indictment tracks the statute and alleges specifically that Defendant "obtain[ed] information from one or more protected computers" through his access to those computers. (Ind. ¶ 14.) Combined with other allegations specifying the approximate timeframe of Defendant's conduct, the Indictment satisfies the pleading threshold imposed by Rule 7. If Defendant is instead arguing that the Government cannot prove that he obtained information, he raises only an evidentiary issue that is insufficient to merit dismissal at this stage. See, e.g., United States v. Coffey, 361 F. Supp. 2d 102, 111 (E.D.N.Y. 2005) ("[T]he validity of an indictment is tested by its allegations, not by whether the Government can prove its case." (citations omitted)).

The court therefore denies Defendant's motion to dismiss based on the claimed failure to allege that he "obtained information."

iv. Failure to Properly Allege Value Lost as a Result of the Scheme Under Section 1030(a)(4)

Defendant's final argument is that the Government fails to establish that the losses from Defendant's alleged scheme totaled more than $5,000 per year, which he claims is required by Section 1030(a)(4). (MTD at 5-6.) Inherent in this argument is the underlying claim that the "object of the fraud and the thing obtained consists only of the use of the computer."[3] 18

[3] Defendant also argues that the Government is required to allege the value of the items obtained through the intrusion and cites several opinions from civil cases regarding Section 1030(a) claims. (See, e.g., Hr'g Tr. at 11-14.) Those opinions do not bear on a criminal prosecution, however. While Section 1030 permits civil actions by parties

U.S.C. § 1030(a)(4). (See also MTD at 5.) The Government responds that it is not obligated to allege a loss amount, as the Indictment alleges that he obtained "objects of value" other than the use of the compromised computers. (Mem. in Opp'n to MTD Mot. ("MTD Opp'n") (Dkt. 27) at 7.)

The Indictment's failure to allege the lost value attributable to the alleged intrusions does not undermine its validity. The plain language of the statute only requires the Government to establish the value of the loss as part of the violation if both the object of the fraud and the thing obtained are limited only to the "use of a computer." 18 U.S.C. § 1030(a)(4). The Indictment alleges that, through Defendant's intrusions, he obtained "information[] and United States and foreign currency" in addition to the "use of a computer." (Ind. ¶ 12).) Other allegations likewise indicate that the alleged fraud's purpose was merely to access computers but also to obtain revenue from the defrauded advertising companies. (Id. ¶ 9.) Crediting the Indictment's allegations, these claims are sufficient to support the charge against Defendant, and the Government is not required at this stage to claim any value attributable to the alleged intrusion.[4]

Accordingly, the court denies Defendant's motion to dismiss based on the claimed failure to allege the value lost as a result of the alleged scheme.

---

suffering loss or damage as a result of that section, the party bringing the action must allege that they have been harmed in one of five ways, including suffering more than $5,000 in aggregate losses over a one year period. See 18 U.S.C. § 1030(g). There is no such predicate imposed on criminal prosecutions, however. Id. § 1030(c).

[4] Defendant additionally argues that the losses alleged must have been suffered by the victim of the intrusion and not solely by a third party (see Reply at 4) and that the "statute is not designed to protect the financial interests of a foreign business" (MTD at 6). Defendant argues that losses suffered by the intended victim of the alleged fraud cannot be counted towards the value of the losses suffered by the alleged victims of the intrusions. (Id. at 4-5.) The court need not address this argument at this point, as the allegation that the objects of the fraud included more than use of the computers obviates the need for any allegation of value lost or gained.

3. Extraterritoriality and Due Process Considerations

Defendant makes two related arguments: first, that the Wire Fraud Counts cannot be applied extraterritorially as a general matter of statutory interpretation; and second, that neither the Wire Fraud nor the Computer Fraud Counts can be applied to him consistent with the Due Process clause of the Fifth Amendment.[5] (See MTD at 7-12.) The court finds that the Wire Fraud Counts do not require an extraterritorial application of the underlying statute, and that neither the Wire Fraud nor the Computer Fraud Counts violate Defendant's rights to due process. Accordingly, Defendant's motion to dismiss those counts is denied.

a. The Presumption Against Extraterritoriality

In support of his claim that the Wire Fraud Counts cannot be applied to conduct abroad, Defendant points to the presumption against extraterritoriality. (MTD at 11.) The presumption against extraterritoriality is a cannon of construction which states that "[a]bsent clearly expressed congressional intent to the contrary, federal laws will be construed to have only domestic application." RJR Nabisco, Inc. v. European Cmty. ("RJR Nabisco II"), — U.S. —, 136 S. Ct. 2090, 2100 (2016) (internal citations omitted). Questions of extraterritoriality are assessed using a "two-step framework:"

> At the first step, we ask whether the presumption against extraterritoriality has been rebutted—that is, whether the statute gives a clear, affirmative indication that it applies extraterritorially. . . . If the statute is not extraterritorial, then at the second step we determine whether the case involves a domestic application of the statute . . . by looking to the statute's "focus." If the conduct relevant to the statute's "focus" occurred in the United States, then the case involves a permissible domestic application even if other conduct relevant to the focus occurred in a foreign country; but if the conduct relevant to the focus occurred in a foreign country, then the case

[5] Neither Defendant nor the Government addressed any statutory or due process concerns associated with the alleged money-laundering conspiracy, though Defendant stated at oral argument that he "would make an argument [regarding the money laundering statute] if the motion to dismiss is not granted." (See Hr'g Tr. at 44). Because the parties have not briefed the issue, the court does not address the money laundering count at this juncture.

> involves an impermissible extraterritorial application regardless of any other conduct that occurred in U.S. territory.

Id. at 2101. Under the second step of this inquiry, courts looking for a statute's "focus" should identify "those transactions that the statute seeks to regulate." Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 267 (2010). Once determined, the court must look to the "territorial events or relationships" implicated by that focus, see Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197, 216 (2d Cir. 2016), and assess whether those events or relationships were located domestically or abroad under the facts before them. If the court finds that the contacts relevant to the focus in the case before it occurred domestically, then that application of the law is not impacted by the presumption against extraterritoriality. Id. ("If the domestic contacts presented by the case fall within the 'focus' of the statutory provision or are the 'objects of the statute's solicitude,' then the application of the provision is not unlawfully extraterritorial." (quoting Morrison, 561 U.S. at 267)).

b. Extraterritoriality of the Wire Fraud Counts

i. Applying the Two-Step Framework to the Wire Fraud Statute

In relevant part, the statute criminalizing wire fraud reads:

> Whoever, having devices or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses . . . transmits . . . by means of wire . . . in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or purpose [shall be deemed to have violated the law].

18 U.S.C. § 1343. The Second Circuit has determined that this language lacks clear indicia of intended extraterritorial application and so does not satisfy the first step of the analysis detailed above. See European Cmty. v. RJR Nabisco, Inc. ("RJR Nabisco I"), 764 F.3d 129, 140-41 (2d Cir. 2014), rev'd and remanded on other grounds, 136 S. Ct. 2090; see also United States v.

Hawitt, No. 15-CR-252 (PKC), 2017 WL 663542, at *4 (E.D.N.Y. Feb. 17, 2017) (applying RJR Nabisco I to a wire fraud prosecution). The panel expressly declined, however, to identify the "focus" of the wire fraud statute, finding instead that the Plaintiffs in that case "alleged [domestic] conduct . . . that satisfie[d] every essential element of the mail fraud . . . claims." RJR Nabisco I, 764 F.3d at 142 & n.14.

The limited number of opinions attempting to discern the "focus" of the wire fraud statute generally break into two camps: those emphasizing the "wires" and those looking to the "fraud." Courts in the first category have largely looked to the Supreme Court's decision in Pasquantino v. United States, 544 U.S. 349 (2005), as their source of authority. In that case, the Court briefly considered whether a wire fraud prosecution alleging a scheme to evade Canadian taxes constituted an impermissible extraterritorial application of that law and held that it did not. Id. at 371. Defendants were convicted of wire fraud based on their use of New York phone lines to order alcohol from another U.S. state, and that alcohol was then smuggled across the Canadian border. Id. at 353. The Court held that application of the wire fraud statute did not violate the prohibition on extraterritoriality, as the "offense was complete the moment [the defendants] executed the scheme inside the United States." Id. at 371. Several subsequent opinions have concluded that this holding dictates that any use of U.S. wires is sufficient to render application of wire fraud statute domestic. See, e.g., United States v. Hayes, 99 F. Supp. 3d 409, 421 (S.D.N.Y. 2015); United States v. Coffman, 771 F. Supp. 2d 735, 738-39 (E.D. Ky 2011).

On the other hand, several recent opinions reviewing the wire fraud statute and the substantially similar mail fraud statute found those statutes' "focus" was the "scheme to defraud." United States v. All Assets Held at Bank Julius, — F. Supp. 3d —, No. 04-CV-798, 2017 WL 1508608, at *15 (D.D.C. Apr. 17, 2017); United States v. Prevezon Holdings, Inc., 122

F. Supp. 3d 57, 71-72 (S.D.N.Y. 2015); see also Elsevier, Inc. v. Grossman, 199 F. Supp. 3d 768, 783-84 (S.D.N.Y. 2016) (concluding the mail fraud statute's focus is on the "particular class of frauds" prohibited in the statute). Drawing from this "focus," one court held that:

> a complaint alleges a domestic application of wire fraud when (1) a defendant or coconspirator commits a substantial amount of conduct in the United States, (2) the conduct is integral to the commission of the scheme to defraud, and (3) at least some of the conduct involves the use of U.S. wires in furtherance of the scheme to defraud.

Bank Julius, 2017 WL 1508608, at *15 (citing Elsevier, 199 F. Supp. 3d at 784).[6]

Considering these competing views, the court concludes that the wire fraud statute's "focus" is the fraudulent scheme. The court respectfully disagrees with the view that Pasquatino requires nothing more than U.S.-based wire transfers to demonstrate domestic application. Pasquantino considered only whether the fact that the ultimate victim of a fraudulent scheme rendered the application of the wire fraud statute impermissible extraterritorial, even though the underlying scheme was otherwise entirely carried out in the United States. Pasquantino, 544 U.S. at 371-72. The Court did not speak to the readily-distinguishable case of a scheme devised and otherwise executed abroad that involves some use of U.S. wires. Instead, the court agrees with the contrary opinion expressed above that Congress's focus in enacting the wire fraud prohibition was to regulate frauds, and not solely a means of perpetrating a fraud. Accordingly, the court analyzes the Indictment using the three-part test set forth in Bank Julius.

[6] While no decision separately addresses the extraterritorial application of the wire fraud conspiracy statute, other courts have concluded that "the extraterritorial reach of an ancillary offense like aiding and abetting or conspiracy is coterminous with that of the underlying criminal statute." United States v. Ali, 718 F.3d 929, 940 (D.C. Cir. 2013) (collecting cases). The court agrees that there is no reason to differentiate the extraterritoriality analysis as between "ancillary" offenses and the underlying substantive offense, and so the court's examination of the wire fraud violation applies equally to the related wire fraud conspiracy count.

ii. Application to the Wire Fraud Counts

Applying this tripartite test, the court concludes that the Wire Fraud Counts requires only domestic application of the underlying statutes, as the "click fraud" scheme was supported in large part by domestic conduct. While the face of the Indictment alleges only a single wire transfer (see Ind. ¶ 19), the Government represented to the court that it intends to present evidence that Defendant leased a server from a New Jersey-based company, which he used to make similar wire transfers in furtherance of the scheme to more than 800 compromised computers in the United States (see MTD Opp'n at 25; Hr'g Tr. at 42). Moreover, the Government provided further detail on the wire transfers themselves, describing how the "user agent string"[7] transfers allowed infected servers to "masquerade" as personal computers. (See Hr'g Tr. at 22-23.) This charade is vital to the alleged scheme, as it gives the victim advertising company the false impression that individual users are "clicking" on its advertisements. Considering both the large number of computers allegedly affected[8] and the importance of the wires to the fraud, the court concludes that the alleged domestic conduct related to the "click fraud" is both "substantial" and "integral to the commission" of the underlying scheme. See Bank Julius, 2017 WL 1508608, at *15.

Accordingly, the court denies the motion to dismiss the Wire Fraud counts based on the presumption against extraterritoriality. Defendant may, however, renew his objection to the

[7] A "user agent string" is a "file 'typically used by a software agent such as a web browser to identify itself . . . by submitting a characteristic identification string to its operating peer.'" (Combined Opp'n at 10 (quoting Compl. (Dkt. 1) ¶ 11 n.6).)

[8] Defendant argues that the court should view the number of servers in the context of the overall number of computers—upwards of 100,000 worldwide—allegedly infected by Defendant's malware. (Reply at 9.) This approach would, however, allow criminal defendants to dilute their responsibility in the United States by engaging in more criminal behavior in other countries. For this reason, the court concludes that the question of whether activity was "substantial" should be viewed objectively and not solely as a percentage of other activity in furtherance of the scheme.

Wire Fraud Counts on this basis at a later time once the Government provides further detail on the alleged domestic conduct in furtherance of the "click fraud" scheme.

4. Alleged Lack of "Nexus" to the United States

Defendant's final argument in favor of dismissal is that the Wire Fraud and Computer Intrusion counts violate his right to due process, as they fail to allege a "nexus" between the acts of which Defendant is accused and the United States. (MTD at 7-8.) In support of this argument, Defendants repeats many of his previous points, arguing that the Indictment fails to allege that he acted within the United States, intended to defraud any U.S. person or company, or obtained anything of value other than the use of U.S.-based computers.

Regardless of congressional intent, federal criminal statutes may only be applied extraterritorially where that application is consistent with due process requirements. United States v. Yousef, 327 F.3d 56, 86 (2d Cir. 2003). This requires showing a "sufficient nexus between the defendant and the United States, so that [extraterritorial] application would not be arbitrary or fundamentally unfair." United States v. Al Kassar, 660 F.3d 108, 118 (2d Cir. 2011) (internal quotation marks and citations omitted). "For non-citizens acting entirely abroad, a jurisdictional nexus exists when the aim of [the charged] activity is to cause harm inside the United States or to U.S. citizens or interests." Id. (internal citation omitted). Due process does not, however, require the defendant to be on notice that they would be "subject to criminal prosecution in the United States so long as they would reasonably understand that their conduct was criminal and would subject them to prosecution somewhere." Id. at 119.

The court finds that application of the charged counts to Defendant is consistent with due process. At the outset, the court notes that the Wire Fraud Counts are not subject to the due process limitations discussed above. As discussed in the preceding section, Defendant's alleged U.S.-based conduct renders application of the wire fraud statute to him domestic, and so he

cannot be said to have "act[ed] entirely abroad." Id. at 118. Moreover, to the extent that the Computer Intrusion Counts seek extraterritorial application of the underlying statute,[9] the acts alleged in those counts were "aim[ed] . . . [at] caus[ing] harm inside the U.S. or to U.S. citizens or interests," sufficient to satisfy due process. Id. at 118. The Indictment alleges that Defendant targeted U.S.-based computers for unauthorized access, compromise, and use in furtherance of the fraudulent scheme. (See, e.g., Ind. ¶¶ 6-7.) While Defendant argues that the ultimate aim of the alleged fraud targeted foreign companies and persons (see MTD Opp'n at 8), that larger aim does not negate the goal of the charged activity: targeting computers in the U.S. for intrusion and exploitation. This alleged purpose is sufficient to satisfy due process limitations on extraterritoriality.

Accordingly, the court concludes that application of the wire fraud and computer intrusion statutes here is consistent with due process and so denies Defendant's motion to dismiss the Indictment on that basis.

* * *

For the foregoing reasons, Defendant's motion to dismiss the indictment is denied in its entirety.

B. Motions for a Bill of Particulars and for Disclosure of Grand Jury Material

Defendant also seeks a bill of particulars and disclosure of grand jury information. Though governed by different standards, Defendant's motions raise substantially similar points.

---

[9] Unlike the wire fraud statute, the statute underlying the Computer Intrusion Counts has the indicia of congressional intent to apply extraterritorially. As noted, the statutory definition of "protected computers" includes computers that are "used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). In adopting this definition of "protected computer," Congress was explicit in its purpose of ensuring that the law penalized "hackers" based outside of the United States, citing examples of foreign individuals who harmed United States computers. See S. Rep. No. 104-357, 1996 WL 492169, at *4 (1996). Viewed against this backdrop, Section 1030 is properly viewed as applying extraterritorially at least to prosecutions of foreign actors whose actions affect "protected computers" in the U.S. See United States v. Ivanov, 175 F. Supp. 2d 367, 374-75 (D. Conn. 2001); cf. also Microsoft, 829 F.3d at 219-20 (relying in part on legislative history to determine a statute's "focus").

First, Defendant argues that the allegation that he "obtained information" through the alleged computer intrusions (Ind. ¶ 14) is inconsistent with the alleged "click fraud" scheme. (See BOP Mot. at 1; GJ Mot. at 1-2.) Second, Defendant contends that there is no support for the alleged connection between the Eastern District of New York and himself, his co-conspirators, or the acts committed in furtherance of the conspiracy. (See BOP Mot. at 2; GJ Mot. at 2-3.)

For the reasons that follow, the court grants in part and denies in part Defendant's motion for a bill of particulars and denies Defendant's motion to unseal grand jury materials.

1. Motion for a Bill of Particulars

In his motion for a bill of particulars, Defendant seeks additional specification regarding (1) the alleged computer intrusions; (2) the conspiracy; (3) the transactions at issue in the money-laundering counts; and (4) the allegedly fraudulent wire transfers and underlying scheme.[10] (See BOP Mot. at 3-4.) In response, the Government argues that Defendant has not shown a need for the requested information and that it has already "disclos[ed] [] nearly all of the requested facts," through the Complaint, Indictment, and discovery.[11] After review of the parties' submissions, the court orders the Government to provide limited additional information regarding the alleged computer intrusions but denies the remaining requests.

a. Legal Standard

The purpose of a bill of particulars is to allow a defendant "to identify with sufficient particularity the nature of the charge pending against him, thereby enabling a defendant to

[10] Defendant also requests a bill of particulars stating whether he is alleged to have participated as a principal or an aider and abettor with regard to each charged count. (See BOP Mot. at 3-4.) In its opposition to the motion, however, Government explicitly states the method of liability charged with respect to each count, mooting that request. (See Mem. in Opp'n to BOP & GJ Mots. ("Combined Opp'n") (Dkt. 39) at 7.)

[11] The Government also argues that Defendant fails to provide "good cause" to support his filing of the motion for a bill of particulars outside of the 14 day window set by Federal Rule of Criminal Procedure 7(f). (Combined Opp'n at 3.) However, the court previously granted Defendant leave to file the motion (May 18, 2017, Min. Entry), and so this argument is not discussed here.

prepare for trial, prevent surprise, and to interpose a plea of double jeopardy." United States v. Bortnovsky, 820 F.2d 572, 574 (2d Cir. 1987). Decisions as to whether or not to grant a bill of particulars are left to "the sound discretion of the district court." United States v. Davidoff, 845 F.2d 1151, 1154 (2d Cir. 1988). Courts are only required to grant a bill of particulars where the charges of the indictment are so general that they do not "advise the defendant of the specific acts of which he is accused." United States v. Chen, 378 F.3d 151, 163 (2d Cir. 2004) (internal quotation marks and citation omitted). Whether this standard is met turns on "whether the information sought is necessary, not whether it is helpful." United States v. Facciolo, 753 F. Supp. 449, 451 (S.D.N.Y. 1990). In making this determination, "the court must examine the totality of the information [already] available to the defendant—through the indictment, affirmations, and general pre-trial discovery." United States v. Bin Laden, 92 F. Supp. 2d 225, 233 (S.D.N.Y. 2000); see also Bortnovsky, 820 F.2d at 574 ("Generally, if the information sought by the defendant is provided in the indictment or in some acceptable alternate form, no bill of particulars is required.").

b. Application to the Categories of Information Sought by Defendant

i. Information Concerning the Alleged Computer Intrusions

Defendant requests specification of both the dates and times of the alleged access to protected computers and the nature and location of the information allegedly obtained as a result of that unauthorized access. (BOP Mot. at 3.) The Government contends that it has provided much of this information through document discovery and early disclosure of expert witness reports, including disclosure of the "manner in which [the malware] infects targeted computers and . . . operates once inside the computers" and the Internet Protocol ("IP") addresses and locations of infected computers. (See Mem. in Opp'n to BOP & GJ Mots. ("Combined Opp'n") (Dkt. 39) at 8-9; Hr'g Tr. at 40-41, 43.)

Despite the insight provided by the Government's existing productions, the court concludes that there remains a risk of unfair surprise that must be mitigated. On the one hand, the categories of material already provided by the Government, particularly the compromised servers' IPs and location information, offer sufficient guidance regarding Defendant's alleged access to those servers. While that information does not directly identify the date and time of Defendant's alleged access, it is sufficient to refine his review of other discovery materials and ensure that he has a fair opportunity to prepare for trial. However, as discussed above, the Indictment alleges that Defendant "obtained information" through his unauthorized access to a protected computer (Ind. ¶¶ 12, 14), but does not elaborate on this claim. Defendant argues persuasively that the information that could be obtained through the "click fraud" scheme is not obvious from the existing allegations. Moreover, Defendant cannot look to other, similar prosecutions for guidance as to this element, as this is a "cutting-edge" case by the Government's own admission. (Hr'g Tr. at 21.) Despite the suggestion that insight into the information allegedly obtained may be gleaned from the Government's expert report disclosures (see Hr'g Tr. at 20-21; Combined Opp'n at 8-9), the court is concerned that, in this unique prosecution, Defendant is effectively unguided as to one of the elements of the Computer Intrusion Counts[12] and so is impaired in his ability to prepare for trial.

Accordingly, the court orders the Government to provide a bill of particulars identifying the categories of information allegedly obtained in connection with the Computer Intrusion Counts.

[12] While Count One, alleging a violation of Section 1030(a)(4), does not necessarily require the Government to prove that a defendant "obtained information," it does require a showing that he or she obtained "anything of value." 18 U.S.C. § 1030(a)(4). Here, the Government alleges that one of the things of value obtained as a result of the intrusion was "information," (Ind. ¶ 12) and so incorporates that "information" into its recitation of the elements.

ii. Conspiracy and Co-Conspirator Information

Defendant seeks several categories of information relating to the conspiracy, including identification of his alleged co-conspirators, the date, time, and location of the conspiracy's initiation, and the overt acts perpetrated in furtherance of the conspiracy charges.[13] (See BOP Mot. 3-4.) In response, the Government points to productions which purportedly provide much of the information requested, including records of payments made to Defendant and other co-conspirators, records associated with the websites maintained by Defendant and his alleged co-conspirators, and payments and communications between the alleged co-conspirators. (Combined Opp'n at 6-7.)

Criminal defendants are not automatically entitled to identification of unindicted co-conspirators. United States v. Follieri, No. 08-CR-850 (JGK), 2009 WL 529544, at *1 (S.D.N.Y. Mar. 3, 2009) (collecting cases). Courts considering requests for co-conspirator identification consider factors including:

> (i) the number of co-conspirators; (ii) the duration and breadth of the alleged conspiracy; (iii) whether the Government otherwise has provided adequate notice of the particulars; (iv) the volume of pre-trial discovery; (v) the potential danger to co-conspirators and the nature of the alleged criminal conduct; and (vi) the potential harm to the Government investigation.

United States v. Nachamie, 91 F. Supp. 2d 565, 572 (S.D.N.Y. 2000). Other details of a conspiracy, including requests for "the nature of the 'wheres, whens, and with whoms'" of a conspiracy, are frequently "held to be beyond the scope of a bill of particulars." United States v. Barret, 824 F. Supp. 2d 419, 439 (E.D.N.Y. 2011) (internal citation omitted) (collecting cases).

[13] Defendant's requests appear to be directed at understanding the basis for the allegation that he and others conspired "within the Eastern District of New York." (See BOP Mot. at 2.) At oral argument, however, the Government clarified that it does not allege that Defendant or his alleged co-conspirators were located in the United States but only that they engaged in conduct in the United States, such as infecting U.S.-based computers with malware and engaging a New Jersey company to host a server for the alleged scheme. (Hr'g Tr. at 45.)

Similarly, "[t]here is no general requirement that the government disclose in a bill of particulars all the overt acts it will prove in establishing a conspiracy charge." United States v. Carroll, 510 F.2d 507, 508-09 (2d Cir. 1975).

The court concludes that the Government's disclosures to date adequately inform Defendant of the information sought through these requests. Many of the factors listed above might, in other circumstances, weigh in favor requiring disclosure of the co-conspirators' identities. However, the information already provided by the Government includes explicit listing of the Defendant's brother as a co-conspirator in the Complaint as well as email and payment records identifying the other alleged co-conspirators by name. (Combined Opp'n at 6-7.) These disclosures obviate the need to further identify those individuals through a bill of particulars. Moreover, Defendant's requests for the overt acts, location, dates, and duration of the conspiracy go beyond the scope of the information to which he is entitled, as they seek the "wheres, whens, and with whoms" of the conspiracy. Barret, 824 F. Supp. 2d at 439; see also United States v. Walker, 922 F. Supp. 732, 739 (N.D.N.Y. 1996) ("[D]etailed evidence of a conspiracy is generally unavailable to defendants through a bill of particulars, and overt acts in furtherance of the conspiracy need not be disclosed.").

For these reasons, the court denies Defendant's request for a bill of particulars specifying additional information regarding the conspiracy and co-conspirators.

iii. Information Regarding the Money-Laundering Conspiracy

Defendant seeks additional information regarding the financial transactions alleged to be part of the money-laundering scheme, and also the "nature, location, source, ownership and control of the proceeds" allegedly laundered. (BOP Mot. at 4.)

The court finds that no bill of particulars is required in light of the existing disclosures. The Government's statement that it has already provided Defendant with the transactions alleged

to constitute money laundering averts the need for a bill of particulars in that regard. Moreover, Defendant's further request for specification of the source of the proceeds is not necessary to understand the charges against him. The Indictment specifies that the purpose of the alleged laundering transactions was to conceal the proceeds of the alleged computer intrusions and wire fraud. (See Ind. ¶ 21.) This limitation appropriately cabins the scope of Defendant's trial preparation and removes the risk of unfair surprise. Cf., e.g., United States v. Stern, No. 03-CR-81 (MBM), 2003 WL 22743897, at *4 (S.D.N.Y. Nov. 20, 2003) (concluding that identification of the wrongful conduct the defendant sought to conceal was necessary to avoid unfair surprise).

Accordingly, the court denies Defendant's motion for a bill of particulars providing further details of the money laundering transactions at issue.

iv. Information Regarding the Wire Fraud

Defendant's final request seeks further information regarding the alleged fraudulent scheme underlying the Wire Fraud Counts. He specifically seeks the time and location of any fraudulent misrepresentations, and the recipients of the "user agent string" that was allegedly transmitted to compromised computers by use of the wires. (See BOP Mot. at 3.)

The court again concludes that existing disclosures by the Government adequately apprise him of the basis for the charges against him. The Government represented that it has provided IP addresses and locations of the 800 computers alleged to have been affected by the malware (Hr'g Tr. at 40), a disclosure which directly answers Defendant's request for information about the recipients of the "user agent string." Further, while the Government has not disclosed the specific times and locations of any fraudulent misrepresentations, Defendant is also apprised of the nature of the alleged misrepresentations through the description of the alleged "click fraud" scheme through the Indictment, the Complaint, and other filings. Combined with the Government's production of payments by the advertising companies

allegedly targeted in that scheme (Combined Opp'n at 6, 11), these descriptions provide Defendant with sufficient information to understand the charges against him, prepare his defense, and avoid unfair surprise at trial.

Accordingly, the court denies Defendant's request for a bill of particulars providing additional information detailing the misrepresentations and wire transmissions underlying the alleged wire fraud.

2. Motion for Disclosure of Grand Jury Material

Defendant moves for an order requiring disclosure of the colloquy to and testimony given before the grand jury that indicted him. Defendant claims that this information is necessary to "support his motion to dismiss and/or cross-examine Government witnesses." (See GJ Mot. at 1.) In support of his motion, Defendant reiterates his need for further information regarding the allegations that he "obtained information" from protected computers and that he entered into a conspiracy that "took place within the Eastern District of New York." (See GJ Mot. at 1-3.) Defendant argues that the grand jury minutes may provide insight into the basis for these allegations, explicitly suggesting that they may have resulted from misrepresentations or omissions by the prosecutor. (Reply in Supp. of GJ Mot. ("GJ Reply") (Dkt. 41) at 2-3; see also Hr'g Tr. at 47-48.)

a. Legal Standard

Rule 6 of the Federal Rules of Criminal Procedure permits courts to "authorize disclosure—at a time, in a manner, and subject to any other conditions that it directs—of grand-jury matter . . . at the request of a defendant who shows that a ground may exist to dismiss the indictment because of a matter that occurred before the grand jury."[14] Fed. R. Civ.

[14] Defendant initially framed his motion as falling under Rule 6(e)(3)(E)(i), which permits disclosure of grand jury material "preliminarily to or in connection with a judicial proceeding." (GJ Mot. at 1.) However, Defendant's

P. 6(e)(3)(E)(ii). Decisions as to whether disclosure is warranted based on those considerations are left to the court's discretion. See In re Petition of Craig, 131 F.3d 99, 104 (2d Cir. 1997).

"[T]he party seeking disclosure [of grand jury materials] must show a 'particularized need' that outweighs the need for secrecy." United States v. Moten, 582 F.2d 654, 662 (2d Cir. 1978). "[R]eview of grand jury minutes is rarely permitted without specific factual allegations of government misconduct." United States v. Torres, 901 F.2d 205, 233 (2d Cir. 1990) (abrogated on other grounds). Defendants do not meet this standard where they "offer little more than speculation that some impropriety may have occurred before the grand jury." United States v. Ordaz-Gallardo, 520 F. Supp. 2d 516, 519 (S.D.N.Y. 2007). Moreover, challenges cannot be based allegations that a grand jury returned a "facially valid indictment" based on "inadequate or incompetent evidence." United States v. Calandra, 414 U.S. 338, 345 (1974); see also United States v. Dunn, No. 05-CR-127 (KMK), 2005 WL 1705303, at *2 (S.D.N.Y. July 19, 2005) (applying Calandra to a motion under Rule 6(e)(3)(E)(ii)).

b. Application

Defendant fails to satisfy the burden of particularized need necessary to obtain review of grand jury materials. At root, Defendant's arguments are based on speculation that the grand jury could not have been convinced to return the charges against him based on the evidence he has reviewed. For instance, he argues that the fact that neither he nor his alleged co-conspirators were alleged to be in New York as incongruous with the allegation that the conspiracy "took place 'in the Eastern District of New York.'" (GJ Mot. at 2.) From this, he conjectures that the

---

motion is based explicitly on his contention that "material misrepresentation of facts as well as crucial omissions may have been made during the proceedings leading to the indictment." (Reply in Supp. of GJ Mot. ("GJ Reply") (Dkt. 41) at 1; Hr'g Tr. at 43.) Accordingly, the court treats Defendant's motion as seeking disclosure based on alleged prosecutorial misconduct before the grand jury and addresses it under the more appropriate standard quoted above.

prosecutor must have provided incomplete disclosures or made material misrepresentations to the grand jury.[15] This speculation is not grounded in any "specific factual allegations," however, and does not merit unsealing that information. Torres, 901 F.2d at 233.

Accordingly, the court denies Defendant's motion to unseal material from the grand jury that indicted him.

III. CONCLUSION

For the foregoing reasons, Defendant's motions to dismiss the indictment and for disclosure of grand jury materials are DENIED WITHOUT PREJUDICE, and his motion for a bill of particulars is GRANTED IN PART and DENIED IN PART. The Government is ORDERED to provide Defendant with a bill of particulars identifying the categories of information alleged to have been "obtained" in connection with the Counts One and Two of the Indictment by no later than June 9, 2017.

SO ORDERED.

s/Nicholas G. Garaufis

Dated: Brooklyn, New York
May 31, 2017

NICHOLAS G. GARAUFIS
United States District Judge

[15] When asked about this point at oral argument, the Government clarified that it alleges only that "there was a significant amount of conduct integral to the scheme which took place [in the United States,] including hundreds of computers that were affected and infected by the malware." (See Hr'g Tr. at 45.)

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

UNITED STATES OF AMERICA

-against-

FABIO GASPERINI,

Defendant.

MEMORANDUM & ORDER

16-CR-441 (NGG)

----------X

NICHOLAS G. GARAUFIS, United States District Judge.

Before the court is Defendant Fabio Gasperini's pre-trial motion to suppress (the "Motion"). (Mot. to Suppress ("MTS") (Dkt. 59). Defendant is charged with two counts of computer intrusion, one count of conspiracy to commit wire fraud, one count of wire fraud, and one count of conspiracy to commit money laundering. (See Indictment (Dkt. 3) ¶¶ 11-21.) Defendant moves to exclude evidence obtained pursuant to (1) warrants issued under the Stored Communications Act (the "SCA"), 18 U.S.C. §§ 2701 et seq; (2) a March 26, 2015, warrant issued by Magistrate Judge Marilyn D. Go; and (3) search warrants executed by Italian law enforcement in Italy. (See generally MTS.) For the following reasons, Defendant's motion is DENIED.

I. BACKGROUND

The court assumes familiarity with the allegations against Defendant, which are discussed at greater length in the court's most recent opinion. (See May 31, 2017, Mem. & Order (Dkt. 45) at 2-3.) Accordingly, the court recites only the facts that are relevant to the present motion.

A. Warrants for Electronic Communications and Related Information

The Government's investigation of Defendant began in 2015. (Gov't Opp'n to MTS ("MTS Opp'n") (Dkt. 71) at 5.) Pursuant to the SCA, the Government obtained multiple search

warrants for Google email accounts associated with Defendant (the "SCA Warrants"). (Id.) In support of the Government's first SCA Warrant application, Federal Bureau of Investigation ("FBI") Special Agent George Schultzel prepared an affidavit (the "Schultzel Affidavit") which included observations by a confidential informant who claimed to have observed computers infected by malicious software. (Id.; see also March 26, 2015, Warrant ("Mar. Warrant"), Ex. A to MTS (Dkt. 59-1) at ECF pp.3-10.) Based on that application, Judge Go issued a warrant (the "March 2015 Warrant") permitting searches of "information associated with 'gaspoplo@gmail.com' that is stored at the premises owned, maintained, controlled, or operated by Google, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, CA 94043." (Mar. Warrant at ECF pp.1, 13.) The Government obtained subsequent five subsequent SCA Warrants. (MTS Opp'n at 5.)

Prior to the issuance of the final SCA Warrant, the Second Circuit issued its decision in In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp. ("Microsoft"), 829 F.3d 197 (2d Cir. 2016). The panel held that the SCA's reach is limited by the presumption against extraterritoriality, such that warrants issued under that act cannot reach data stored on servers located outside of the United States. Id. at 220-22. Responding to the sole post-Microsoft warrant, Google stated that its production in that instance included only responsive records stored on U.S. servers. (Google Ltr., Ex. B. to MTS Opp'n (Dkt. 71-2).)

B. Searches by Italian Authorities

The Government provided information related to the present prosecution to Italian law enforcement officials in June 2016. (MTS Opp'n at 6.) The Government also requested that Italian authorities conduct a search of Defendant's home in Italy. (Id.) Italian law enforcement conducted the search with FBI agents present. (Gov't Sur-Response to MTS Opp'n (Dkt. 85) at 1.)

II. DISCUSSION

Defendant asks the court to suppress all evidence obtained pursuant to (1) the SCA Warrants; (2) the March 2015 Warrant specifically; and (3) searches conducted by Italian law enforcement. (See MTS at 1-2.) In the alternative, Defendant requests an evidentiary hearing pursuant to Franks v. Delaware, 438 U.S. 154 (1978), to evaluate alleged misstatements in the Schultzel Affidavit. (MTS at 1.) The court addresses these elements of the Motion in turn and concludes that Defendant is not entitled to any of the relief sought.

A. Information Obtained Pursuant to the SCA Warrants

Defendant argues that all information obtained from foreign servers controlled by Google, including Defendant's emails and other information, must be suppressed based on the Microsoft decision. (MTS at 2-5.) The court concludes that, even taken as true, Defendant fails to provide facts that would justify suppression of any evidence obtained in violation of the SCA and dismisses the Motion on that ground.

1. The SCA and the Microsoft Decision

The SCA provides privacy protection for, inter alia, certain electronic communications in the possession of third parties that provide communications services to the public ("service providers").[1] See, e.g., Orin S. Kerr, A User's Guide to the Stored Communications, and a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208, 1213 (2004). Among its many provisions and protections, the SCA limits the Government's ability to require service providers to disclose their users' content and information. See 18 U.S.C. § 2703. As relevant here, the Government may compel service providers to disclose the contents of users' electronic

[1] Specifically, the SCA refers to two different types of service providers: providers of electronic communications services and providers of remote computing services. See Orin S. Kerr, A User's Guide to the Stored Communications, and a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208, 1214 (2004). While the protections afforded by the SCA sometimes vary based on the type of service provider at issue, that distinction is not relevant to consideration of the motion at hand.

communications by obtaining a warrant that complies with the Federal Rules of Criminal Procedure. Id. § 2703(a), (b)(1)(A).

In Microsoft, the Second Circuit held that (1) the SCA's warrant provisions do not apply extraterritorially; and (2) the SCA does not permit issuance and enforcement of a warrant against U.S.-based service providers to obtain contents of electronic communications stored abroad. Microsoft, 829 F.3d at 222. With respect to the second of these points, the court found that the SCA's "focus" was on the "privacy of stored communications." Id. at 217. From this, the panel determined that "the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed—here, where it is seized by Microsoft, acting as an agent of the government." Id. at 220. Accordingly, the court concluded that "execution of [a warrant seeking data stored outside the United States] would constitute an unlawful extraterritorial application of the act." Id.

2. Defendant's Objection to the SCA Warrants

Defendant argues that the Second Circuit's decision in Microsoft requires suppression of all information obtained in reliance on the SCA Warrants. In support of this contention, Defendant states that he "lived in Italy at all times, making it more than likely that the vast majority of [Defendant's] emails and information was stored in Google's foreign servers."[2] (MTS at 5.) The Government argues that Defendant provides neither a sufficient factual nor legal basis for suppression. (MTS Opp'n at 6-12.) The court concludes that Defendant is not

[2] Defendant makes the separate but related argument that the extraterritorial application of the SCA should be limited by "principles of international comity." (Reply in Supp. of MTS ("MTS Reply") (Dkt. 78) at 4-6.) This argument is beside the point in the current context, however. The extraterritorial reach of the SCA is already limited by Microsoft, and the relevant question is whether evidence obtained in violation of that limitation must be excluded.

entitled to suppression, as he alleges at most a statutory violation of the SCA that does not require exclusion of evidence.

Statutory violations of the SCA, without more, are not remedied through exclusion of the resulting evidence in court. The text of the SCA itself states that "[t]he remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter." 18 U.S.C. § 2708. The SCA's enumerated remedies do not include suppression,[3] and numerous courts have held that defendants claiming only statutory violations of the SCA are not entitled to exclusion of the collected evidence. See, e.g., United States v. Scully, 108 F. Supp. 3d 59, 88 (E.D.N.Y. 2015) (collecting cases); United States v. Guerrero, 768 F.3d 351, 358 (5th Cir. 2014); United States v. Powell, 444 F. App'x 517, 520 (3d Cir. 2011) (unpublished opinion).

While Defendant argues that the Government's alleged violations of the SCA amounted to violations of his Fourth and Fifth Amendment rights (Reply in Supp. of MTS ("MTS Reply") (Dkt. 78) at 7-8), his arguments in support of this assertion are unavailing. The Fourth Amendment has no application to searches conducted abroad where the subject is a foreign national who lacks substantial or voluntary connections to the United States. See United States v. Verdugo-Urquidez, 494 U.S. 259, 274-75 (1990); see also In re Terrorist Bombings of U.S. Embassies in E. Africa (Fourth Amendment Challenges), 552 F.3d 157, 168 (2d Cir. 2008) (stating that, under Verdugo-Urquidez, "the Fourth Amendment affords no protection to aliens searched by U.S. officials outside of our borders"). As Defendant has consistently emphasized, he lacked any connection to the United States prior to his extradition into this country. (See, e.g.,

[3] The SCA provides for both civil and criminal remedies. See 18 U.S.C. §§ 2701(b), 2707; see also United States v. Scully, 108 F. Supp. 3d 59, 88 (E.D.N.Y. 2015).

Mot. to Dismiss (Dkt. 9) at 7.) As such, he cannot claim that searches of his data stored outside the U.S. violated his Fourth Amendment rights. Though the Fifth Amendment does apply to foreign nationals prosecuted in the United States, see, e.g., In re Terrorist Bombings of U.S. Embassies in E. Africa (Fifth Amendment Challenges), 552 F.3d 177, 199-200 (2d Cir. 2008), Defendant raises no colorable argument that the use of evidence obtained in reliance on the SCA Warrants violates his rights under that amendment. He points only to the Microsoft opinion's language regarding the "focus" of the SCA (see MTS at 8), which contemplated the presumption against territoriality (a canon of statutory construction) without discussing any constitutional considerations.[4]

Accordingly, the court concludes that suppression is not warranted as to evidence obtained in reliance on the SCA Warrants.

B. Objections to the March 2015 Warrant

Defendant separately argues that evidence obtained pursuant to the SCA Warrants, and particularly the March 2015 Warrant, should be suppressed because the Government engaged in outrageous conduct that "shock[s] the conscience" in violation of the Due Process Clause.[5] (See

[4] Defendant also argues that the SCA Warrants did not extend to information stored abroad, pointing to the statement in the warrant that it extended to all information related to the subject email address "that is stored at premises owned, maintained, controlled, or operated by Google, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, CA 94043." (MTS at 5; see also Mar. Warrant at ECF p.13.) Defendant states that the warrant should not be read to extend to data stored abroad, "as historically 'warrants' issued by U.S. judges do not run to other countries," and so the Government's use of that warrant to obtain data stored outside of the U.S. was unreasonable. (MTS at 6.) However, the language of the warrant does not suggest the geographic limitation proposed by Defendant, and other courts appear to have treated warrants with similar language as applying to data controlled by the warrant's recipient, regardless of the location of the data. See, e.g., In the Matter of the Search of Information Associated with [Redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc., — F. Supp. 3d —, No. 16-MJ-757 (GMH), 2017 WL 2480752, at * (D.D.C. June 2, 2017) ("The Warrant makes no mention of the location of the Google server or servers on which the records . . . are stored . . . "); In re Information Associated with One Yahoo email address that is Stored at Premises Controlled by Yahoo, No. 17-M-1234, No. 17-M-1235; 2017 WL 706307, at *2 (E.D. Wis. Feb. 21, 2017) ("In neither [warrant] application does th[e] government state that it knows where the data sought might be stored, although both state that it is possible that some of the information sought may be stored on servers located outside of the United States.")

[5] Defendant also argues at one point that the court should exclude the evidence in the exercise of its "supervisory powers," but he does not present any separate arguments in support of that point. (See MTS at 6.)

MTS at 6-17.) Defendant alleges various transgressions by the Government and the confidential information cited in the Schultzel Affidavit (the "CI"):

> (1) the Government relied solely on a confidential informant that was never established as reliable;
>
> (2) the confidential informant was not competent, let alone an expert;
>
> (3) the confidential informant deliberately misrepresented material facts with a reckless disregard for the truth;
>
> (4) the confidential informant based conclusions on uncorroborated assumptions based on facts never established;
>
> (5) the Government never bothered to verify or corroborate the confidential informant's false factual premises and conclusions;
>
> (6) the Government was present with Italian authorities when the defendant's residence in Rome, Italy was searched and evidence was seized, but still has refused to turn over the Italian search warrant in discovery; and
>
> (7) the Government enlisted Italian authorities to act as their agents.

(Id. at 7.) Alternatively, Defendant requests a hearing pursuant to Delaware v. Franks, 438 U.S. 154 (1978), regarding the March 2015 Warrant, which he claims was improperly obtained through misrepresentations and misstatements by the CI and FBI in the Schultzel Affidavit. (Id.) The court concludes that neither suppression nor an additional evidentiary hearing is merited.

1. Outrageous Government Conduct

Defendant first contends that the Government's conduct during the investigation merits suppression of all evidence obtained in connection with the SCA Warrants. Under very limited circumstances, government conduct in the course of an investigation may violate a Defendant's right to due process and require suppression of evidence or even dismissal of claims. See, e.g., United States v. Rahman, 189 F.3d 88, 131 (2d Cir. 1999). "[O]nly Government conduct that 'shocks the conscience' can violate due process." Id. (citation omitted). Defendants bear the

burden of proving outrageous government conduct, United States v. Cromitie, 727 F.3d 194, 221 (2d Cir. 2013), and that burden is "very heavy," Rahman, 189 F.3d at 131. "Generally, to be 'outrageous,' the government's involvement . . . must involve either coercion or a violation of the defendant's person." United States v. Al Kassar, 660 F.3d 108, 121 (2d Cir. 2011). Relief based on outrageous government conduct is reserved for the most extreme examples. See, e.g., United States v. Chin, 934 F.2d 393, 398-99 & n.4 (2d Cir. 1991) (citing "[e]xtreme physical coercion" and "psychological torture" as potential examples of outrageous government conduct).

Defendant falls well short of the required showing. Even if credited, Defendant's allegations—that the Government presented an affidavit that contained affirmative misstatements by the CI, failed to verify the CI's allegations, participated in a foreign law enforcement search, and failed to provide the foreign warrant in discovery—do not constitute the kinds of "coercion or violation of the defendant's person" that may form the basis for a claim of outrageous government conduct. Moreover, many of Defendant's allegations of misconduct in connection with obtaining the warrant are better considered under the Franks framework, discussed below. Accordingly, Defendant's request to suppress evidence based on outrageous government conduct is denied.

2. Objections to the March 2015 Warrant Affidavit

Defendant moves the court to conduct a hearing to address alleged misstatements and omissions in the Schultzel Affidavit, which he alleges undercut the required showing of probable cause as to the March 2015 Warrant. (See MTS at 8.) Submitted in connection with the March 2015 Warrant application, the Schultzel Affidavit lists statements made by "a confidential source working with the FBI," including the CI's observations of infections of servers with malware and steps taken by the infected servers thereafter. (Mar. Warrant at ECF pp.3-4, ¶¶ 5-9.) Schultzel also states his own understanding, based on his "knowledge, training, and experience," that these

operations were "typically used to further 'click fraud.'" (Id. at ECF p.4 ¶ 8.) Defendant claims that the Schultzel Affidavit contains multiple "deliberately false" statements by the CI and provides two affidavits purporting to support his allegations. (See MTS at 8.) Defendant further contends that the failure by Schultzel himself to identify both those alleged misstatements, as well as two typos in the affidavit, shows that he did not corroborate the CI's information though independent investigation. (Id. at 15.)

a. The Franks Standard for Challenging Warrant Applications

Where a defendant claims that a warrant was secured by an inaccurate or misleading affidavit, the court's consideration is guided by the framework set by Franks v. Delaware. Under that framework, evidence may be suppressed if the defendant shows that: "(1) the claimed inaccuracies or omissions are the result of the affiant's deliberate falsehood or reckless disregard for the truth; and (2) the alleged falsehoods or omissions were necessary to the [issuing] judge's probable cause . . . finding." United States v. Rajaratnam ("Rajaratnam III"), 719 F.3d 139, 146 (2d Cir. 2013) (internal quotation marks and citation omitted). Under the second prong of the test, courts must determine whether "setting aside the falsehoods, what remains of the affidavit is insufficient to support a finding of probable cause." United States v. Coreas, 419 F.3d 151, 155 (2d Cir. 2005). "Omissions are governed by the same rules as misstatements," Rajaratnam III, 719 F.3d at 146 (internal quotation marks and citations omitted); however, "[a]n affiant cannot be expected to include . . . every piece of information gathered in the course of an investigation. . . . [and] Franks protects [only] against omissions that are designed to mislead, or that are made in reckless disregard of whether they would mislead, the magistrate," United States v. Awadallah, 349 F.3d 42, 67-68 (internal quotation marks and citation omitted).

Suppression motions based on Franks are properly addressed through an evidentiary hearing in which "the defendant is entitled . . . to test the veracity of the affiant's statements."

United States v. Falso, 544 F.3d 110, 125 (2d Cir. 2008). However, a defendant is not automatically entitled to such a hearing and must first make a "substantial preliminary showing" that the two prongs of the Franks test are satisfied. Id. But see United States v. Rajaratnam ("Rajaratnam I"), No. 09-CR-1184 (RJH), 2010 WL 3219333, at 1 & n.1 (S.D.N.Y. Aug. 12, 2010) (concluding that Franks requires a substantial preliminary showing only as to the first prong of the analysis but acknowledging that the Second Circuit "has assumed" the showing must be made as to both prongs). In order to make this "substantial preliminary showing":

> [T]he challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine. There must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof. They should point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons. Affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained. Allegations of negligence or innocent mistake are insufficient.

Franks, 438 U.S. at 171.

b. Application

While Defendant alleges at least six separate misstatements or omissions, only two merit discussion and neither warrants an evidentiary hearing. First, Defendant points to the statement that the CI observed a file downloaded by the malware "repeatedly issuing commands that would effect a click on an ad . . . ." (See Mar. Warrant at ECF p.6 ¶ 8 (emphasis added).) Defendant presents an affidavit from a purported information technology expert stating that "there is no repetition for this click fraud task in the script" and that the CI's statement to the contrary "is deliberately false." (Wong Aff., Ex. B to MTS (Dkt. 59-2) ¶ 33.) Defendant argues that the absence of repetition undercuts the probable cause determination, as the issuance of repeated commands would lead a "reasonably prudent Magistrate [to] believe that criminal activity was

ongoing." (MTS at 11.) Whether there was repetition is irrelevant,[6] however: evidence of any click command in furtherance of the fraud would provide probable cause to believe a crime was committed. Defendant does not allege that there was no click command, and so his argument on this point fails to satisfy the second prong of the Franks test.

Defendant also alleges that the Schultzel Affidavit misleadingly omits details concerning the connection between the malware and Defendant's computer. (MTS at 12.) The Schultzel Affidavit states that the server "pushing" one of the files downloaded onto infected computers originated from a computer in Italy. (See Mar. Warrant at ECF p.6 ¶ 7.) Defendant argues that this statement misleadingly suggests that the Italian computer was the "source" of the file or the "host" of the central control panel that issued commands to infected servers. (See MTS at 12.) On this point, Defendant fails to satisfy the first prong of the Franks standard. While Defendant contends that admittedly accurate statements in the Schultzel Affidavit should have been accompanied by a non-criminal alternate explanation or elaboration, he offers no basis to conclude that this omission was "designed to mislead, or [] made in reckless disregard [of its potential to] mislead, the magistrate." Awadallah, 349 F.3d at 68 (internal quotation marks and citation omitted).

The other misstatements and omissions alleged by Defendant do not fit within the Franks framework. Defendant cites several omissions without suggesting that they render the affidavit erroneous or misleading, instead implicitly attacking the magistrate judge's finding of probable cause absent any wrongdoing by the affiant. (See MTS at 8 (identifying failure to assert basis for CI's reliability); id. at 9-10 (challenging the CI's expertise based on information not referenced

[6] In its opposition, the Government insists that "there [was] repetition" but appears to concede that the repetition may have been manually directed and not automatic, as suggested by the affidavit. (MTS Opp'n at 14.)

in the affidavit); id. at 13-15 (suggesting an alternate, non-criminal explanation for certain information connecting Defendant to the click fraud).) Defendant also points to two typos and misplaced "boilerplate" language in the affidavit that he alleges demonstrate that the FBI did not independently corroborate the information contained therein. (Id. at 15-17.) These errors do not appear to be intentional or reckless misstatements, however, and so do not merit suppression. See Franks, 438 U.S. at 171 ("Allegations of negligence or innocent mistake are insufficient.").

For the foregoing reasons, Defendant's motion for a Franks hearing is denied.

C. Information Obtained from Italian Law Enforcement

Defendant separately seeks suppression of all information gathered by Italian police on the basis that those officers were acting as "agents" of the Government in a scheme "designed to evade constitutional requirements."[7] (MTS at 18.) Defendant's argument is rooted in an Italian law enforcement report, which describes a search warrant executed at Defendant's residence in Rome. (Id.) The report states that two FBI agents were present for the search. (Id.; see also Italian Warrant, Ex. D to MTS (Dkt. 59-4); Bertollini Aff., Ex. E to MTS (Dkt. 59-5) ¶¶ 4-8.)

Defendant's argument is meritless. As previously noted, the Fourth Amendment does not apply to searches abroad that target persons, such as Defendant, who lack substantial or voluntary connections to the United States. Verdugo-Urquidez, 494 U.S. at 275-76. This is the case even where the search is conducted directly by U.S. agents. Id. For the same reason, the Fourth Amendment's exclusionary rule does not apply to the fruits of those searches, including

[7] Defendant also asks the court to compel the Government to provide copies of the Italian search warrant used in the search of Defendant's apartment. (MTS at 17-18.) The Government states that it is not in possession of the search warrant (MTS Opp'n at 16), and notes that Defendant has apparently been in possession of the Italian search warrant left with Defendant's family in Rome "since at least June 7, 2017," (Sur-Response to MTS (Dkt. 85) at 1-2). While Defendant continues to insist that he should have received additional documents connected to the Italian law enforcement searches (Sur-Reply to MTS (Dkt. 87)), the Government's representation that it does not have the requested documents is sufficient to defeat any motion to compel. See United States v. Lee, 723 F.3d 134, 141 (2d Cir. 2013) (holding defendant was not entitled to foreign law enforcement documents that were "not even within the 'government's possession, custody, or control.'" (quoting Fed. R. Crim. P. 16(a)(1)(E)).

where that evidence is seized by foreign law enforcement officials. See, e.g., United States v. Defreitas, 701 F. Supp. 2d 297, 304 (E.D.N.Y. 2010); United States v. Vega, No. 07-CR-707 (ARR), 2012 WL 1925876, at *4-5 (E.D.N.Y. May 24, 2012). Given that the same evidence would not be subject to suppression if it were seized directly by U.S. officials, Defendant plainly cannot seek exclusion on the basis that Italian law enforcement officers were acting as the Government's "agents."[8]

III. CONCLUSION

For the foregoing reasons, Defendant's motion to suppress (Dkt. 59) is DENIED.

SO ORDERED.

s/Nicholas G. Garaufis

Dated: Brooklyn, New York
July 13, 2017

NICHOLAS G. GARAUFIS
United States District Judge

[8] Defendant separately contends that "evidence seized aboard should be suppressed because the Italian authorities expressly recognized that it belongs to [Defendant's brother], and not to Defendant." (MTS at 18.) Defendant does not explain why this would necessitate suppression, however.

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

UNITED STATES OF AMERICA,

-against-

FABIO GASPERINI,

Defendant.

MEMORANDUM & ORDER

16-CR-441 (NGG)

----------X

NICHOLAS G. GARAUFIS, United States District Judge.

Defendant Fabio Gasperini is charged with two counts of computer intrusion, one count of conspiracy to commit wire fraud, one count of wire fraud, and one count of conspiracy to commit money laundering. (See Indictment ("Ind.") (Dkt. 3) ¶¶ 11-21.) The charges stem from Defendant's alleged creation of a "botnet" to further a "click fraud" perpetrated against advertising companies. (Id. ¶¶ 1-10.) Stated briefly, the Government alleges that Defendant and others obtained unauthorized access to computers in the U.S. and around the world and remotely directed those computers to fraudulently inflate the number of times that online advertisements were "viewed." The court assumes familiarity with the allegations against Defendant, which are discussed in previous opinions. (See, e.g., May 31, 2017, Mem. & Order (Dkt. 45) at 2-3.)

Defendant has filed numerous motions in limine seeking exclusion of certain proposed trial evidence. (1st Mot. in Lim. ("1st MIL") (Dkt. 65); 2d Mot. in Lim. ("2d MIL") (Dkt. 105); 3d Mot. in Lim. ("3d MIL") (Dkt. 111).) For the reasons set forth below, Defendant's motions in limine are GRANTED IN PART and DENIED IN PART, with ruling on certain questions RESERVED until trial.

I. LEGAL STANDARD

A. Motions in Limine

"The purpose of a motion in limine is to allow the trial court to rule in advance of trial on the admissibility and relevance of certain forecasted evidence." Gorbea v. Verizon N.Y., Inc., No. 11-CV-3758 (KAM), 2014 WL 2916964, at *1 (E.D.N.Y. June 25, 2014) (citing Luce v. United States, 469 U.S. 38, 40 n.2 (1984); Palmieri v. Defaria, 88 F.3d 136, 141 (2d Cir. 1996); Nat'l Union Fire Ins. Co. of Pittsburgh v. L.E. Myers Co., 937 F. Supp. 276, 283 (S.D.N.Y. 1996)). "Evidence should be excluded on a motion in limine only when the evidence is clearly inadmissible on all potential grounds." United States v. Paredes, 176 F. Supp. 2d 179, 181 (S.D.N.Y. 2001). "[C]ourts considering a motion in limine may reserve decision until trial, so that the motion is placed in the appropriate factual context." Jean-Laurent v. Hennessy, 840 F. Supp. 2d 529, 536 (E.D.N.Y. 2011) (citing Nat'l Union Fire Ins. Co., 937 F. Supp. at 287). Further, a district court's ruling on a motion in limine is preliminary and "subject to change when the case unfolds." Luce, 469 U.S. at 41. The moving party bears the burden of establishing that evidence is inadmissible for any purpose and so properly excluded on a motion in limine. See United States v. Pugh, 162 F. Supp. 3d 97, 101 (E.D.N.Y. 2016).

B. Relevance and Prejudice

The admissibility of evidence at trial is determined by the Federal Rules of Evidence, and only relevant evidence may be admitted. Fed. R. Evid. 402. Evidence is relevant if it "has any tendency to make a fact more or less probable" and "the fact is of consequence in determining the action." Fed. R. Evid. 401. This standard imposes a "very low" bar. United States v. White, 692 F.3d 235, 246 (2d Cir. 2012) (quoting United States v. Al-Moayad, 545 F.3d 139, 176 (2d Cir. 2008)). Even where it is determined to be relevant, evidence may be excluded if the court determines that "its probative value is substantially outweighed by a danger of one or

more of the following: unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence." Fed. R. Evid. 403.

II. DEFENDANT'S MOTIONS

A. Objections to Expert Testimony and Other Testimony

1. Testimony Regarding Cybercrime, Botnets, and Malware

In its initial notice of proposed expert witnesses, the Government stated that it expected to call an expert[1] to testify regarding:

> general terminology related to cybercrime, including botnets, click fraud scripts, malware, servers, the Shellshock vulnerability and other terms material to the charges against the defendant. In addition, the government anticipates that [the expert witness] will testify about the operation and capabilities of botnets and malware generally as well as the operation and capability of the malware and botnet employed by the defendant in this case.

(See May 23, 2017, Gov't Ltr. ("Expert Disclosure Ltr.") (Dkt. 38) at 2.) Defendant raises three general objections to this proposed testimony, which are discussed separately below.

a. Background Testimony Regarding Cybercrime, Botnets, and Malware

Defendant first contends that general testimony providing background regarding cybercrime, botnets, and malware is irrelevant and may prejudice or confuse the jury. (1st MIL at 1-2.) The court disagrees. Despite its sometimes tenuous relationship to "disputed matter," background evidence and testimony is "universally offered and admitted as an aid to understanding" and treated as relevant. See Fed. R. Evid. 401 advisory committee notes. While the proffered expert testimony here does not directly implicate the allegations against Defendant,

[1] The Government initially stated that this testimony would be provided by either Ovie Carroll or Joe Variani. (See May 23, 2017, Gov't Ltr. ("Expert Disclosure Ltr.") (Dkt. 38) at 2.) Defendant objected on the grounds that this testimony could be provided by other witnesses. (1st MIL at 1.) In its response, the Government agreed with Defendant's position and stated that the testimony will instead be provided by Dr. Johannes Ulrich, who was also previously noticed as an expert witness. (Gov't Opp'n to 1st MIL ("MIL Opp'n") (Dkt. 93) at 8.)

it provides background regarding the sometimes obscure technology and concepts at issue in the case, including malware, botnets, and server operations, and other terms that are likely to be unfamiliar to the average juror. The court views this proposed testimony as relevant and helpful, and sees no overriding potential for prejudice or confusion evident at this juncture. Defendant's motion to exclude background testimony regarding cybercrime, malware, botnets, and related terms and concepts is therefore DENIED.

b. Testimony Regarding the Capabilities of the Botnet and Malware Allegedly Employed by Defendant

Defendant next argues that testimony regarding the capabilities of the specific malware and botnet that he allegedly employed is both irrelevant and more prejudicial than probative. (1st MIL at 2.) Defendant contends that testimony regarding those capabilities without further context does not touch on the actual employment of malware and botnet alleged to have occurred in this case and so is not consequential to the action. (Id.) The Government responds that it will limit the expert testimony to the actual capabilities of the botnet at issue, which it argues are relevant to the "value" obtained as a result of the alleged computer intrusions. (Gov't Opp'n to 1st MIL ("MIL Opp'n") (Dkt. 93) at 8-9.) The Government's proposed basis for introducing testimony establishes that the proffered evidence is clearly relevant, as it goes directly to the elements the Government must prove to secure a conviction on the charged counts. See, e.g., (stating that computer intrusion must lead to obtaining "anything of value"). To the extent that Defendant argues that testimony regarding general botnet capabilities risks prejudicing or confusing jurors by presenting them with far-flung harms, the Government appears to address this concern by limiting the testimony to "the capabilities of the specific botnet that defendant built, and not [] capabilities that are merely speculative." (MIL Opp'n at 8.) Defendant's motion to exclude testimony the capabilities of his alleged botnet and malware is therefore DENIED.

c. Hearsay

Lastly, Defendant contends that the proposed testimony is hearsay because the Government does not state that the expert has personally reviewed the malware, botnet, or servers at issue here. (1st MIL at 2.) In response, the Government clarifies that the expert has, in fact, viewed the malware at issue. (MIL Opp'n at 9.) Based on this representation, Defendant's motion to exclude testimony regarding the malware and botnets is DENIED.

2. Testimony of Dr. Johannes Ulrich

Defendant moves to limit the testimony of Dr. Johannes Ulrich, which the Government states will cover:

> [Ulrich's] review of findings from one of SANS' "honeypots," i.e., a computer security mechanism used to research online and computer- based threats and identify means to better protect against such threats. . . . [as well as] his observations that certain Network Attached Storage devices were being targeted through the Shellshock vulnerability.

(Expert Disclosure Ltr. at 1-2.)

Similar to the previous motion, Defendant moves to exclude testimony regarding "computer-based threats and the means to protect against such threats," claiming that this general testimony is irrelevant to the allegations against him. (1st MIL at 4.) The Government has clarified that Ulrich's testimony will be specific to "how he detected the defendant's malicious software (using a detection mechanism called a 'honeypot') and his analysis of that malicious software." (MIL Opp'n at 10.) Presented in this way, the proposed testimony analyzing the malware at issue is clearly relevant to the charges against Defendant. Accordingly, Defendant's motion to exclude that testimony is DENIED.

Defendant separately moves to limit Ulrich's testimony to exclude references to servers from which the Government does not allege information was obtained. (1st MIL at 4.)

Defendant argues that testimony is irrelevant because he "has not been charged with attempt, and therefore an attempted intrusion is not an element of any of the charges." (Id.) However, as the Government points out, several of the counts include charges of attempt. (MIL Opp'n at 10-11 (citing Ind. ¶¶ 12, 14, 19).) Testimony regarding observations of alleged attempts are thus directly relevant to the charges against Defendant. Defendant's motion to exclude testimony regarding servers from which no information or other objects of value were obtained is therefore DENIED.

3. Testimony of Stuart Gorton

Defendant seeks to exclude the testimony of Stuart Gorton on the basis that "he is not an expert." (1st MIL at 3.) The Government's initial list of potential expert witnesses included Gorton. (See Expert Disclosure Ltr. at 2.) In response to Defendant's motion, however, the Government states that it "presently intends to call Mr. Gorton as a fact witness."[2] (MIL Opp'n at 9.) Defendant's motion to exclude Gorton's testimony is DENIED as moot.

4. Italian Linguists

In its expert disclosure, the Government informed Defendant that it would seek to introduce testimony from Italian linguists regarding their own translations or the accuracy of others' translations of Italian language documents. (Expert Disclosure Ltr. at 3.) Defendant argues that the court should exclude the testimony of the linguists, as their identities have not been disclosed to Defendant, preventing him from assessing their qualifications. (1st MIL at 7.) After Defendant filed his motion, the Government disclosed the names of its proposed linguist witnesses (Gov't Witness List (Dkt. 109) at 4), and indicated that it will "elicit their

[2] The Government states, however, that it "reserves the right to call Mr. Gorton as an expert." (MIL Opp'n at 9.) If the Government seeks to adduce expert testimony from Gorton, Defendant may renew his motion to exclude Gorton's expert testimony at that time.

qualifications during direct testimony" (MIL Opp'n at 13). In light of this disclosure, the court DENIES Defendant's motion to exclude the linguists' testimony as moot.

5. Testimony Regarding the New Jersey Server

Defendant seeks exclusion of proposed testimony analyzing a server allegedly operated by Defendant in connection with the charged computer intrusions. (1st MIL at 3-4.) He contends that the Government "constructively denied" him access to that server by failing to provide access to "forensic tools" that Defendant claims are needed to view the contents of the server. (Id. at 4.) The court already considered and rejected the same argument in the context of Defendant's motion to compel. (See July 6, 2017, Hr'g Tr. (Dkt. 96) 21:6-25.) Defendant has received access to the "virtual image file" containing the contents of that server, as well as reports by Government witnesses analyzing the file. (Id. 19:6-22.) There has therefore been no constructive denial of access, and the motion to exclude testimony regarding the contents of the server on that basis is DENIED.

B. Objections to Documentary and Electronic Evidence

1. Italian Language Documents

Defendant seeks exclusion of "all [] documents in a foreign language for which a certified translation has not been provided." (1st MIL at 7.) The Government's response does not indicate whether it has provided Defendant with copies of certificated translations of all proposed foreign language trial exhibits. To the extent that it has not already done so, the Government is ORDERED to provide Defendant with any certified translations that it seeks to introduce at trial by no later than July 22, 2017. Any foreign language documents for which certified translations are not provided by this deadline will be held inadmissible at trial.

2. Defendant's Emails

Defendant moves to exclude the entire contents of email accounts attributed to Defendant. (1st MIL at 4-6.) He argues that those documents have not been properly authenticated and, separately, that they constitute inadmissible hearsay.[3] The court addresses these points separately.

a. Authentication

Defendant first argues that the emails should be held inadmissible, as they have not been and cannot be properly authenticated. (Id. at 5.) Defendant contends that email communications can only be authenticated by testimony of the author or another party who observed the drafting and sending of the message. (Id.) The Government counters that authentication of emails can and will be provided through circumstantial evidence.[4] (MIL Opp'n at 11.)

"Under Federal Rule of Evidence 901(a), the burden rests on the proponent of documentary evidence to provide 'sufficient evidence to support a finding that the matter in question is what the proponent claims.'" Bell v. Rochester Gas & Elec. Co, 329 F. App'x 304, 306 (2d Cir. 2009) (summary order) (quoting Fed. R. Evid. 901(a)). "The proponent carries his burden by introducing 'sufficient proof . . . [allowing] a reasonable juror [to] find in favor of authenticity.'" Id. (quoting United States v. Ruggiero, 928 F.2d 1289, 1303 (2d Cir. 1991) (internal quotation marks omitted; alterations in original). "[P]roof of authentication may be direct or circumstantial." Al-Moayad, 545 F.3d at 172. "The proponent need not rule out all

[3] Defendant also claims that the Government "intends to introduce entire email accounts allegedly belonging to Defendant" at trial and argues that "the majority of these . . . emails are grossly irrelevant" and should therefore be excluded. (1st MIL at 4-5.) In response, the Government clarifies that it "does not intend to offer entire email accounts into evidence." (MIL Opp'n at 11.)

[4] The Government does not state what circumstantial evidence it intends to provide to authenticate those documents. The Government's brief does state, however, that it intends to "demonstrate, through subscriber records and the contents of the accounts, that the accounts belong to the defendant" for hearsay purposes. (MIL Opp'n at 11.)

possibilities inconsistent with authenticity, or to prove beyond any doubt that the evidence is what it purports to be." United States v. Gagliardi, 506 F.3d 140, 151 (2d Cir. 2007) (internal quotation marks and citation omitted).

The court is unaware of any authority that authentication of emails can only come through a witness with direct knowledge of the drafting, and Defendant provides none. Rather, courts considering the admissibility of electronic documents and communications have held that "'evidence may be authenticated in many ways' and 'the type and quantum of evidence necessary to authenticate [electronic sources] will always depend on context.'" United States v. Ulbricht, 79 F. Supp. 3d 466, 487-88 (S.D.N.Y. 2015) (quoting United States v. Vayner, 769 F.3d 125, 133 (2d Cir. 2014)). The court concludes that the Government may authenticate the emails through circumstantial evidence and DENIES the motion to exclude those emails.

b. Hearsay

Defendant next objects that emails from the accounts attributed to him must be excluded as inadmissible hearsay. (1st MIL at 5-6.) Defendant's argument is misplaced, however. Leaving aside the authentication question noted above, emails sent by Defendant are admissible for their truth as statements of a party-opponent. See Fed. R. Evid. 801(d)(2)(A). While the same reasoning does not apply to emails received by Defendant, those messages may be introduced for a purpose other than the truth of the matters asserted, such as providing context for Defendant's emails. See, e.g., United States v. Dupree, 462 F.3d 131, 136-37 (2d Cir. 2006). Without knowing the particular emails proffered or the purpose for which the Government seeks

their introduction, the court cannot conclude that they must be excluded.[5] Accordingly, the court RESERVES DECISION on Defendant's motion to exclude emails as inadmissible hearsay.

3. Email Accounts of Alleged Co-Conspirators

Defendant moves to exclude emails from accounts associated with Defendant's alleged, uncharged co-conspirators. (1st MIL at 6.) He argues that those statements do not satisfy the requirements of the co-conspirator exception to the hearsay rule, as the Government can only prove the existence of the conspiracy based on the hearsay itself. (Id. at 6-7.) The Government responds that, as an initial matter, it will establish the existence of the conspiracy through Defendant's own admissions.[6] (MIL Opp'n at 12.)

Under the Federal Rules of Evidence, out of court statements made by a party's co-conspirator "during and in furtherance of the conspiracy" may be introduced for their truth against that party. Fed. R. Evid. 801(d)(2)(E). The proponent of the statements must demonstrate by a preponderance of the evidence both the existence of a conspiracy between the declarant and the party and that the statement was in furtherance of that conspiracy. Bourjaily v. United States, 483 U.S. 171, 175-76 (1987). "[W]hile the hearsay statement itself may be considered in establishing the existence of the conspiracy, there must be some independent corroborating evidence of the defendant's participation in the conspiracy." United States v. Gigante, 166 F.3d 75, 82 (2d Cir. 1999) (internal quotation marks and citation omitted). The degree of corroboration needed may vary depending on the degree to which the hearsay evidence

[5] To the extent that either party seeks to introduce out-of-court statements for a purpose other than the truth of the matter asserted, the opposing party may object at that time and request that the court issue an appropriate limiting instruction to the jury.

[6] The Government also states that it will offer co-conspirator statements as responses to Defendant's own statements as "context" for his emails. (MIL Opp'n at 12.) This purpose does not implicate hearsay concerns because the relevance of the emails is not based on the truth of the matters asserted therein. See Dupree, 462 F.3d at 136-37 (holding that emails offered for context are not subject to exclusion as hearsay).

implicates the defendant in the conspiracy. See United States v. Padilla, 203 F.3d 156, 162 (2d Cir. 2000).

At this stage, the court lacks sufficient information to predetermine the admissibility of co-conspirator statements. In as much as Defendant's position is that the Government cannot prove a conspiracy based solely on his co-conspirators' hearsay statements, that position is effectively rebutted by the Government's assertion that it will offer Defendant's own statements to lay the foundation for the existence of a conspiracy. The Government's representation alone is not, however, sufficient to demonstrate that it will be able to prove the existence of a conspiracy involving Defendant by a preponderance of the evidence. Accordingly, the court RESERVES DECISION on objections to the admission of co-conspirator statements until such time as those statements are offered.

4. Evidence Obtained From Hard Drives Seized Abroad

Defendant seeks exclusion of hard drives seized from his apartment in Italy. (1st MIL at 9.) Defendant first attacks the admissibility of those items based on their relevance and potential prejudice, arguing that the Government has failed to show that the hard drives were in fact Defendant's and contending that they in fact belonged to his brother, an uncharged co-conspirator. (Id.) Even if the court were to accept Defendant's factual contention, however, Defendant points to no authority requiring automatic exclusion of evidence obtained from the possession of another individual, much less an alleged co-conspirator.

Defendant separately argues that evidence obtained from the hard drives should be excluded because "the government failed to produce any evidence of a proper chain of custody." (1st MIL at 9.) This challenge, too, fails. So long as the Government meets its burden of authenticating the hard drives, challenges to chain of custody go only to the weight of the evidence. U.S. v. Shellef, 732 F. Supp. 2d 42, 81 (E.D.N.Y. 2010) (collecting cases). Here, the

Government represents that it will authenticate the hard drives through the testimony of an Italian law enforcement officer involved in their seizure (MIL Opp'n at 14), and so the court finds no reason to exclude the hard drives based on chain of custody.

Accordingly, Defendant's motion to exclude the hard drives is DENIED.

5. Italian Advertising Company Documents

Defendant argues that records from an Italian advertising company, LeonardoADV, produced in discovery should be excluded because "no reasonable juror would consider [those records to be] reliable." (1st MIL at 8.) Defendant bases this contention on the absence of letterhead, addresses, date, preparer's name, and other details in those records. (Id.) Defendant's argument appears to be that these records cannot be authenticated. In response, however, the Government represents that it has obtained a foreign business records certification from LeonardoADV and that it will call an employee of that company as a witness "to further authenticate and explain the records." (MIL Opp'n at 14.) These measures are more than sufficient to authenticate the document under Rule 901. See Fed. R. Evid. 901(b)(1) (stating that authentication may be provided by testimony of a knowledgeable witness). Accordingly, Defendant's motion to exclude those records is DENIED.

C. Objections to Website Printouts

1. Objections to Internet Archive Printouts

Defendant contends that the court should exclude copies of websites generated through the Internet Archive. (1st MIL at 9-11.) Through a service called the "Wayback Machine," the Internet Archive "allows parties to visit digitally archived Web pages," viewing a particular website as it appeared on a given day. Deborah R. Eltgroth, Best Evidence and the Wayback Machine: Toward a Workable Authentication Standard for Archived Internet Evidence, 78 Fordham L. Rev. 181, 185-86 (Oct. 2009). Defendant argues that printouts of archived websites

are inadmissible, as they cannot be properly authenticated. (1st MIL at 9-11.) In response, the Government states that it will authenticate the printouts through in-person testimony by an employee of the Internet Archive "who will explain the nature and creation" of records in that database. (MIL Opp'n at 15.)

Defendant primarily relies on Novak v. Tucows, Inc., No. 06-CV-1909 (JFB) (ARL), 2007 WL 922306 (E.D.N.Y. Mar. 26, 2007), for support. Examining proffered Internet Archive printouts, the court in that case concluded that the documents were insufficiently authenticated under Rule 901 of the Federal Rules of Evidence.[7] Id. at *5. Noting that the archived website data in the Internet Archive was provided by third parties, the court concluded that "information posted on the Wayback Machine is only as valid as the third-party donating the page decides to make it—the authorized owners and managers of the archived websites play no role in ensuring that the material posted in the Wayback Machine accurately represents what was posted on their official websites at the relevant time." Id. Because the proponent of the printouts "proffer[ed] neither testimony nor sworn statements attesting to the authenticity of the contested web page exhibits by any employee of the companies hosting the sites from which plaintiff printed the pages," the court reasoned that the information could not be sufficiently authenticated. Id.

Subsequent to the Novak decision, several courts have concluded that the authentication issues raised in that opinion may be addressed through affidavits from Internet Archive employees. See, e.g., Foster v. Lee, 93 F. Supp. 3d 223, 231-32 (S.D.N.Y. 2015); Martin Trans. Ltd. v. Plattform Advert. Inc., No. 14-CV-2464, 2016 WL 1718862, at *1-2 (D. Kan. Apr. 29,

[7] The court also held that several of the printouts constituted inadmissible hearsay, as they contained articles or other statements sought to be admitted for their truth. Novak, 2007 WL 922306, at *5. This portion of the Novak holding does not appear to be at issue here, as the Government states that it "does not intend to offer [the printouts] for their truth, but merely as a representation of what appears on a particular website at a particular time." (MIL Opp'n at 16.)

2016). One court allowing authentication by this route implicitly acknowledged that the language in Novak would likely require authentication by the website owner, but concluded that "Novak failed to take into account [] the nature of the third party donating the page. . . . [which] simply takes a snapshot of a website at a particular point in time." Abu-Lughod v. Calis, No. 13-CV-2792, 2015 WL 12746198, at *2 (C.D. Cal. May 20, 2015). That court concluded that authentication concerns could be addressed by an "affidavit of a person with personal knowledge who can attest that the third-party crawler operates to create an unaltered copy of a website as it appears on a given day is sufficient to authenticate evidence from the Wayback Machine." Id.

The court finds that testimony from an Internet Archive employee may be sufficient to address the authentication issues noted by Novak. Without knowing the substance of that testimony, however, the court cannot properly assess the authentication of the proffered copies of websites. Accordingly, the court RESERVES DECISION on Defendant's motion to exclude web archive printouts pending testimony purporting to authenticate those documents at trial.

2. Objections to Website Printouts

On the same basis as his objection to the Internet Archive printouts, Defendant moves to exclude printouts of websites not generated through that website. (1st MIL at 11.) In response, the Government states that it will offer the testimony of an individual who "personally captured the website (by printing it or taking a screenshot) at the time that he viewed the website." (MIL Opp'n at 16.) The proposed testimony directly addresses the authenticity of the proffered evidence. Defendant's motion is therefore DENIED.

D. Objections to Inflammatory Language

Defendant seeks an order precluding the Government from stating that either computers or advertisers in the U.S. were "victimized" by Defendant's alleged malware and scheme. (1st

MIL at 11-13.) Defendant argues that U.S. computers were not "victimized" because the information allegedly obtained from them was "worthless." (Id. at 11-12.) Similarly, he argues that U.S. advertisers were not "victims" because the Government does not allege that Defendant obtained from them anything with "market value." (Id. at 12-13.) Defendant's arguments on this point are unavailing. Defendant's argument in favor of excluding the terms "victim" and "victimized" is, in essence, based on the merits of his case: he argues that the allegations against him do not show that he violated the relevant statutes. The Government is within its rights to take and advocate for a different view of the evidence. Moreover, the court does not view the use of the challenged terms as unduly prejudicial in light of the issues being tried. Cf. MF Global Holdings Ltd., — F. Supp. 3d —, 2017 WL 663565, at *5 (S.D.N.Y. Feb. 3, 2017) ("[C]ourts often prohibit the use of certain pejorative terms when such categorizations were inflammatory and unnecessary to prove a claim and such statements do not bear on the issues being tried." (internal quotation marks and citations omitted)). Accordingly, Defendant's motion to exclude the use of "victim" or "victimized" as to computer and advertisers in the United States is DENIED.

E. Objection to References to Certain Advertising Companies

Defendant moves for an order barring evidence or testimony referring to an enumerated list of U.S. companies and government agencies. (2d MIL at 1.) He states that those companies were not mentioned in the discovery material, and seeks exclusion of any mention of those entities "to avoid unfair surprise, confusion of the parties and issues, and to avoid unfair prejudice to Defendant." (Id.) Defendant does not, however, elaborate on the prejudice that he anticipates suffering as a result of mentions of these companies, and so fails to satisfy his burden of making a pre-trial showing that the evidence must be excluded. See Pugh, 162 F. Supp. 3d at 101. Defendant's motion to exclude references to those companies is therefore DENIED.

F. Motion to Allow Defendant to Appear in Civilian Clothes

Defendant requests an order permitting him to appear at trial in civilian clothing and without any restraints. (1st MIL at 13.) The Government does not object. (MIL Opp'n at 16.) Defendant's motion to appear in civilian clothing and without restraints is GRANTED.

G. Objections to Business Records and Records Certifications

1. Business Records and Certification by Linode, LLC

Defendant challenges as deficient the business records certification and underlying records provided by Linode, LLC, a virtual private server provider based in New Jersey. (3d MIL at 2-3.) Certifications of domestic business records are governed by Federal Rule of Evidence 902, which states that records of regularly conducted activities, as defined by Rule 803(6)(A)-(C), are self-authenticating when they are accompanied by "a certification of the custodian or another qualified person that complies with a federal statute or a rule prescribed by the Supreme Court." Fed. R. Evid. 902(11). In turn, Rule 803(6) states that records of regularly conducted activities are not subject to the prohibition on hearsay evidence where:

> (A) the record was made at or near the time by—or from information transmitted by—someone with knowledge;
>
> (B) the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit;
>
> (C) making the record was a regular practice of that activity;
>
> (D) all these conditions are shown by the testimony of the custodian or another qualified witness, or by a certification that complies with Rule 902(11) . . .; and
>
> (E) the opponent does not show that the source of information or the method or circumstances of preparation indicate a lack of trustworthiness.

Fed. R. Evid. 803(6). Defendant argues that the Linode business records and certification are deficient in multiple respects, which the court addresses separately below.

a. Probative Value of the Terms of Service

Defendant asserts that the business records sought to be introduced include records of Defendant's alleged violations of Linode's terms of service. (3d MIL at 2.) Defendant contends that "the probative value of the [terms of service] records is very low, and it is substantially outweighed by the risk of prejudice." (Id.) He does not, however, offer any support for this cursory objection or describe the record at issue. The court finds that Defendant has not satisfied his burden of demonstrating that the records should be excluded at this stage. Accordingly, Defendant's motion to exclude records reflecting violations of the terms of service is DENIED.

b. Virtual Image of the Linode Server

Defendant argues that the "virtual image of the server allegedly leased to [Defendant]" is not a business record because that file was not created in the regular course of business. (Id.) Instead, Defendant alleges that the virtual image was created at the Government's behest. (Id. at 2-3.) If credited as factually accurate, Defendant's assertions may be meritorious. See, e.g., Park W. Radiology v. CareCore Nat'l LLC, 675 F. Supp. 2d 314, 331 (S.D.N.Y. 2009) (holding that business records exception is not available as to a "unique document not kept in the regular course of business"). However, Defendant fails to offer any support for his assertion that the document is not created in the normal course of business. Without further information, the court cannot determine the circumstances under which Linode created the "virtual image" or assess whether it is a "record [] kept in the course of a regularly conducted activity" by that company. See Fed. R. Evid. 803(6)(C). Accordingly, the court DENIES Defendant's motion to exclude the virtual image file. Defendant may renew his objection at trial, and the court will consider the admissibility of the challenged evidence outside the hearing of the jury.

c. Lack of Trustworthiness

Defendant next challenges the admission of Linode's business records and certification on the basis that Linode was "hacked" on multiple occasions and so its records may "demonstrate a lack of trustworthiness." (3d MTD at 3.) Trustworthiness is the "principal precondition to admission" under the business records exception. Saks Intern., Inc., v. M/V Export Champion, 817 F.2d 1011, 1013 (2d Cir. 1987). That requirement is generally measured by the circumstances under which the record was prepared, and is frequently cited as a basis for excluding accident or other unusual activity reports which raise concerns about self-serving testimony. See, e.g., United States v. Kaiser, 609 F.3d 556, 574 (2d Cir. 2010) ("The purpose of the rule is to ensure that documents were not created for 'personal purpose[s] . . . or in anticipation of any litigation' so that the creator of the document 'had no motive to falsify the record in question.'" (citation omitted)).

While, read most generously, Defendant's argument could be seen as raising general arguments about the trustworthiness of the data to be introduced against him, the concerns he raises are not those contemplated by the rule. Issues with data security do not go to whether documents prepared from that data are self-serving, but instead are properly viewed as going to the weight that should be accorded to the resulting records. Accordingly, Defendant's motion to exclude records produced by Linode for lack of trustworthiness is DENIED.

d. Confrontation Clause

Defendant contends that introduction of the Linode records at trial would violate his Confrontation Clause rights under the Sixth Amendment. (3d MIL at 3.) Defendant's argument appears to be essentially derivative of his other points: the records to be introduced against him are "testimonial" because they were made in response to investigation, and not in the normal course of business. (Id.) However, as noted above, Defendant fails to provide the court with any

indication as to the basis for his contention that Linode's records were not created in the regular course of business. (See supra Section II.G.1.b.) Absent further support for his contentions, the court cannot conclude at this time that the records are testimonial and so precluded.[8] Cf. United States v. Feliz, 467 F.3d 227, 236 (2d Cir. 2006) ("[W]here a statement is properly determined to be a business record . . . it is not testimonial . . . even where the declarant is aware that it may be available for later use at trial.") Accordingly, Defendant's motion to exclude Linode's records for violation of the Confrontation Clause is DENIED.

2. Foreign Business Records Certifications

Defendant also raises numerous challenges to foreign business records certifications offered by the Government in connection with certain of its proffered exhibits. (See 3d MIL at 3-8.) Foreign business records certifications offered in a criminal case are governed by 18 U.S.C. § 3505. That section mirrors the requirement of Federal Rule of Evidence 803(6), stating:

> a foreign record of regularly conducted activity . . . shall not be excluded as evidence by the hearsay rule if a foreign certification attests that:
>
> (A) such record was 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) such record was kept in the course of a regularly conducted business activity;
>
> (C) the business activity made such a record as a regular practice; and
>
> (D) if such record is not the original, such record is a duplicate of the original;

[8] Defendant's argument also assumes that the creator of the records will not testify at trial and be subject to cross-examination, which would cure any Confrontation Clause concerns. See Crawford v. Washington, 541 U.S. 36, 59 n.9 (2004) ("[W]hen the declarant appears for cross-examination at trial, the Confrontation Clause places no constraints at all on the use of his prior testimonial statements.")

> unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness.

18 U.S.C. § 3505(a).

a. Italian Law Enforcement Records

During discovery, the Government produced received from Italian law enforcement that provide "a summary of business record information." (MIL Opp'n at 13; 1st MIL at 7-8.) The Government states that it will introduce the underlying business records through foreign business records certifications, while separately introducing the law enforcement summary of those records through testimony by an Italian law enforcement officer. (Id.) However, Defendant states he has not received any certifications from the businesses that provided Italian law enforcement with the underlying records (3d MIL at 4), nor is the court able to locate such certifications in own review of the docket. The Government is ORDERED to advise the court as to whether those certifications have been provided to Defendant by July 22, 2017. The court RESERVES DECISION on the Defendant's motion to exclude those documents at this time.[9]

b. FastWeb and Vodafone Certifications

Defendant moves to exclude business records certifications provided by Vodafone and FastWeb on the ground that they were not timely provided in compliance with 18 U.S.C. § 3505(b). (3d MIL at 5-6.) That subsection states that "at arraignment or as soon after the arraignment as practicable, a party intending to offer in evidence under this section a foreign record of regularly conducted activity shall provide written notice of that intention to each other party." 18 U.S.C. § 3505(b). Defendant errs in proposing that automatic exclusion should result from the Government's purported delay. "The remedy for a violation of Section 3505(b) is to

[9] Defendant also objects that the lack of certain details on the face of the law enforcement summary demonstrates that those records lack sufficient indicia of authenticity (1st MIL at 7-8) or trustworthiness (3d MIL at 4.) For the same reasons stated as to the advertising company records and Linode's business records (see supra Sections II.B.5, II.G.1.c), the court DENIES Defendant's motion to exclude the law enforcement summaries on those bases.

object at trial on the ground of prejudice resulting from the violation." See United States v. Newell, 239 F.3d 917, 921 (7th Cir. 2001). At this point, Defendant has not demonstrated any prejudice resulting from the claimed delay by the Government.

Defendant also seeks exclusion of those certifications on the basis that "[i]t is unclear what business records [those] certification[s] purport[] to authenticate." (3d MIL at 5-6.) Defendant has not, however, articulated why this necessitates exclusion. Defendant's motion to exclude the FastWeb and Vodafone certifications is therefore DENIED.

c. Triboo Media SRL Certification

Defendant argues that the certification provided by Triboo Media SRL ("Triboo") should be excluded because of the informality of that document, which consists of a handwritten certification provided on notebook paper. (3d MIL at 6.) Defendant argues that "[t]he circumstances of execution of this 'certification' indicate a lack of trustworthiness." (Id.) The "trustworthiness" requirement of Section 3505 is commonly read in conjunction with the same requirement imposed by Federal Rule of Evidence 803(6). See, e.g., United States v. Ross, 33 F.3d 1507, 1515 (11th Cir. 1994); United States v. Ekiyor, 90 F. Supp. 3d 735, 737 n.3 (E.D. Mich. 2015). As previously discussed, the trustworthiness element of Rule 803(6) is concerned with whether the information sought to be admitted was prepared under circumstances that suggest self-serving or biased testimony. (See supra Section II.G.1.c.) Defendant's argument regarding the informality of the certification does not implicate those concerns.

Defendant also seeks to exclude the Triboo certification on the basis that it is unclear which records that certification purports to certify. As previously discussed (see supra Section II.G.2.b), Defendant has not provided any justification for seeking exclusion on that basis.

Defendant's motion to exclude the Triboo certification is DENIED accordingly.

d. TopHost Certification

Defendant moves to exclude the certification provided by the Italian company TopHost on the basis that there is no indication that the employee who executed that certification was authorized to make the representations therein. (3d MIL at 7.) Defendant argues that this demonstrates that the records were not prepared "in the course of a regularly conducted activity." (Id.) This argument is misplaced, however: by its terms, Section 3505 requires that the records underlying the certification must be the result of a regularly conducted business activity. See 18 U.S.C. § 3505(a)(1)(B). The statute separately states that the certification itself must be provided by the "custodian of [the record] or another qualified person." Id. at § 3505(c)(2). As such, there is no requirement that the certification must be prepared in the course of a regularly conducted business activity. Defendant does not provide any reason to believe that the underlying records were not prepared in the course of a regularly conducted activity. Furthermore, Defendant does not provide a basis to conclude that the employee who executed the challenged certification was not qualified to do so. Accordingly, Defendant's motion to exclude the TopHost certification is DENIED.

e. Arnoldo Mondadori Editore Certification

Defendant objects to the certification provided by Arnoldo Mondadori Editore on the same grounds discussed in the previous section: he states that the certification was signed by an "employee," potentially indicating that the certification was conducted outside the course of regularly conducted activity. (3d MIL at 8.) This argument fails for the same reasons stated in the previous section. (See supra Section II.G.2.d.)

In addition, Defendant reiterates his earlier argument that the certification should be excluded because it is unclear what records it purports to certify. As noted in previous sections

(see supra Section II.G.2.b), Defendant provides no justification for excluding the records certification on that basis.

Accordingly, Defendant's motion to exclude the Arnolodo Mondadori Editore certification is DENIED.

f. PayPal Europe Records

In addition to challenging foreign business certifications, Defendant argues that the records produced by PayPay Europe demonstrate that the money laundering conspiracy count against him is "frivolous." (3d MIL at 3.) In particular, he argues that those records reflect less than a total of $10,000 in transactions, which he states "do[es] not reach the statutory . . . threshold for extraterritorial application of the money laundering statute." (Id. at 4.) While Defendant makes the cursory argument from this point that the court should "sua sponte" dismiss the money laundering conspiracy count (3d MIL at 4), he does not offer any factual or legal support for his contentions. These bare assertions are far from sufficient to merit dismissal. Defendant's motion to dismiss the money laundering conspiracy count is DENIED accordingly.

H. Continuing Objections

Defendant requests that the court issue an order stating that "all evidentiary objections made in [his] in limine motion [are] deemed objections under all applicable provisions of the U.S. Constitution," and that the court will consider any denied motions in limine as continuing objections at trial. (1st MIL at 13.) The Government argues that this constitutes an "improper attempt to circumvent the law of waiver" and argues that "[D]efendant must articulate the basis for his objections in order to preserve them." (MIL Opp'n at 17.) The court agrees: Defendant cannot duck his obligation to make timely objections by stating that all previous arguments should be treated both as continuing and as raising all available constitutional protections. See United States v. Hall, 348 F.2d 837, 843 (2d Cir. 1965) (emphasizing the need to "clearly and

distinctly alert[] the trial judge, and opposing counsel, to every claim intended to be reserved for possible appeal"); cf. also Fed. R. Crim. P. 51(b) ("A party may preserve a claim of error by informing the court—when the court ruling or order is made or sought—of the action the party wishes the court to take, or the party's objection to the court's action and the grounds for that objection." (emphasis added)). As noted, the court's decision on motions in limine are preliminary, and Defendant may renew his objections as "the case unfolds." Luce, 469 U.S. at 41. The court will not, however, relieve Defendant of his obligation to raise specific objections by revisiting previous motions sua sponte.

III. CONCLUSION

For the foregoing reasons, Defendant's motions in limine (Dkts. 65, 105, 111) are GRANTED IN PART and DENIED IN PART, with ruling on certain questions RESERVED until trial.

SO ORDERED.

s/Nicholas G. Garaufis

Dated: Brooklyn, New York
July 21, 2017

NICHOLAS G. GARAUFIS
United States District Judge

collected by Mr. Reccoppa and returned to you at the beginning of the next trial day. You are not to share your notes with each other, they are for your personal use only. In addition, if you need to take a break when we are not normally taking a break, just raise your hand and either I or one of the parties will see you and we will take a short break at that point.

And that does it. At this point, I thank you for your attention. This case will require very careful attention on the part of the jury, as do all cases, and we all appreciate the fact that you will give it your full attention at all times. At this time, we will begin with opening statements. The first opening statement will be provided by the Government.

Ms. Wells, you may deliver your opening statement on behalf of the Government.

MS. WELLS: Thank you, Your Honor.

OPENING STATEMENT

BY MS. WELLS:

MS. WELLS: The defendant, Fabio Gasperini, is a hacker and a thief. He broke into tens of thousands of computers around the world, from Brooklyn to Bangkok and everywhere in between. He took control of those computers. He programmed them to follow his orders. He stole information from them and he used those computers to commit fraud. He did all of this sitting behind his own computers, halfway around

THE COURT: You'd like to see it.

What's the question?

Q The question is isn't it true that with respect to this bot net, you declare that: It is not a full-fledged command and control server in that it doesn't appear to send any commands, nor does it track the system, look for updates, from the bot. Right now, I don't think that is happening.

Is that accurate?

A It's probably accurate. That's what I said at the time. I don't remember the exact statement.

Q If this article came out on December 15 and in this article you're saying that these bots, these infected QNAP devices don't go anywhere, can these infected QNAP make any click through the botnet?

A This was a day or so after, yes, at that time it's very likely that the command control server was shut down.

Q So, by December 15, if there's no control banner, there's no click from the traffic device, correct?

A Correct.

Q You say during your direct examination that the Shellshock vulnerability won't harm QNAP device, correct?

A Correct.

Q Are you aware that many of the QNAP owners have not patched the device?

A Correct, many of them have not patched the device.

something.
A I can highlight on the screen here.
THE COURT: If you just point on the screen, you will get an arrow.
THE WITNESS: Okay. Thanks.
THE COURT: Go ahead.
Q Can you show me on this script here the part that downloads EMME and CL from the 23 server?
A This is not shown here on this screen shot.
Q It is not shown?
A No.
THE COURT: Is it somewhere else?
THE WITNESS: It was already downloaded. This is when I ran the script the second time.
Q So you analyzed this and you counting up parts?
A I didn't count off parts. These are just parts that didn't run here. This is also run in a laboratory, so --
Q So you are saying that the EMME script did not run in this instance?
A In this instance, it did not get downloaded. It ran, actually. It did not get downloaded.
Q So in this instance, it did not download EMME and CL. And you have a QNAP device; correct?
A Correct.
Q I am going to withdraw. You have a QNAP device?

A Correct.
Q And you say that the script will download EMME and CL; correct?
A Yes.
Q And you will execute the files?
A Uh-hum.
Q And the system will be cleaned up at the end, correct?
A Some of these files will be removed.
Q You just say that in your QNAP test the EMME script didn't execute; correct?
A I ran this test two weeks ago or three weeks ago in the lab for -- and --
Q You did not execute. Okay.
MS. KOMATIREDDY: Objection, Your Honor.
THE COURT: Sustained.
Please don't over speak the witness' answer. Go ahead.
Q Isn't it possible then that other QNAP devices downloaded the script and did not execute EMME or CL?
A It is possible that some were not able to download it. But we definitely observed that at the time that QNAP device downloaded.
Q So you are saying that it is possible that they didn't download or execute EMME; correct?
A Correct.

Q And if it didn't download or execute EMME, there is no click; correct.
A Correct. If the file is not available to them, then....
Q Let me ask you this, if you have a QNAP device and you open the shadow file, if the user request is not in the shadow file, what would you consider the QNAP? Infected or not infected?
A Well, if the QNAP user is not present in the shadow file then -- sorry, the request user is not present in the shadow file, it would not be infected by this particular bot.
Q Not be infected by this bot. And you say the malware created and opened SSH 26; correct?
A Correct.
Q So if you have a QNAP device that doesn't have that part open, would that QNAP be infected or not infected by this particular virus?
A It will probably not be infected.
THE COURT: Okay. We have reached five o'clock and we will break for the day and resume at 9:30 tomorrow morning. I am going to remind you about something I said at the beginning. You will hear it again and again. We are going to adjourn now for the day. Before we do, let me remind you that it is extremely important that you follow my instruction that you not discuss this case with anyone, not your family, friends, or business associates, and not your fellow jurors.

Q Yesterday you say that within the EMME script you found a file called CL; correct?
A Correct.
Q And you say that the CL steals users and passwords the way that the satellite would do; correct?
A Correct.
Q So what happens if CL gets into a QNAP, what kind of user and password would the virus steal?
A If the virus is not pressing, then it will not steal any users and passwords.
Q So if the file related to the cable or the satellite is not in the QNAP, it will not take it?
A Correct.
Q And did you just say that you can't watch cable or satellite directly from the QNAP?
A Correct.
Q Yesterday you also talk about port scanning. Do you remember?
A I probably did, yeah.
Q Now, when you do a port scanning, does the software access any ports?
A It depends on how the port scan is configured, but typically it does access a large number of ports.
Q When you do the ports scan, does the software scanning the internet enter into any port? Does it access any port,

the scanner?
A Yes, it may access any port. That's up to the user to configure.
Q So you're saying that it is called a scanner but it actually intrudes ports?
A It connects to the port and checks if there is a response coming back.
Q So it connects to the port? It doesn't access the port?
A Correct.
Q And when it connects to the port, does it damage it or not?
A No. Typically it does not damage it.
Q Is it illegal to scan the internet in your expert opinion?
A I'm not a lawyer, but I don't believe it is.
Q When the script is run in the QNAP device, it executes a number of comments; correct?
A Correct.
Q These comments change the VNS; correct?
A Correct.
Q Creates the port on SSH 26; correct?
A Correct.
Q And installs the backdoor?
A Yes.
Q It patches?

MR. BERTOLLINI: Six pages.
THE COURT: Does the Government know what six pages we are talking about?
MS. KOMATIREDDY: We are just waiting for it to come up on the screen.
MR. BERTOLLINI: I can describe it.
THE COURT: Just show it to the Government. We are making some changes on the screens right now.
Q Before we look at your notes again, yesterday you talk about the backdoor; correct?
A Correct.
Q And the backdoor is exo.cgi; correct?
A Correct. I believe the file is originally named armgH.cgi, but they were renamed into exo.cgi.
Q Yes. That's what you --
A That's why I called the notes the web backdoor.
Q And if that -- if the specific QNAP were to have the I-686 architecture, it would be gh.cgi; correct?
A Correct. There are different names for different architectures.
Q Okay. Now, I want to show you your notes.
THE COURT: Are these in evidence?
MS. KOMATIREDDY: No, Your Honor.
THE COURT: Okay.
Q So here we have -- one second. Page 1, we have right

here armgH.cgi?
A I do not see anything.
THE COURT: How is that? Do you have it?
THE WITNESS: Got it.
Q Do you see it now?
A I do see the notes now. Let me see if I see -- okay.
Q ArmgH.cgi, this would be the file of the backdoor if the QNAP were to have the arm-based architecture; correct?
A Correct.
Q In your notes here you put the armgH is an IRC bot; correct?
A Actually, the .cgi is the IRC bot. The armgH is not the IRC bots.
Q Yesterday you say that these notes were wrong?
A These notes are notes I took while I was investigating the final reporting.
Q So while investigating --
THE COURT: He has to finish before you start and you have to finish before he starts. That's the way it works, because the court reporter can't take down what you are both saying at the same time. It is a physical impossibility. That much I know. Everybody has to cooperate and the jury is not going to hear everything.
Let's continue.
Q Okay. When you were investigating this, you figured that

armgH was an IRC bot; correct?

A Can you point -- that was my assumption at the time, yes.

(Continued on following page.)

BY MR. BERTOLLINI:
Q And on what basis did you make that assumption?
A I typically look at strings in a file. I may have also uploaded it to a site called VirusTotal that does a quick analysis of the file.
Q Yesterday you said that you did not examine the back door, correct?
A I did not examine in detail the armgH file. I probably just did that, I uploaded it to the -- to VirusTotal.
Q So how did you later determine that armgH is not an IRC bot?
A Based on the report I got from VirusTotal and based on strings, it did not appear to be an IRC bot.
Q So you wrote the note before running the file through the software?
A Correct, I wrote these notes as I was reading this file.
Q Okay. So, if someone is now using that software, he might be likely to believe it is an IRC bot as you did.
A Sorry?
Q If someone is now running the file with the same software, he might be inclined to believe at first impression that that's IRC bot.
A That's possible, yes.
Q Let's move on to Page 3 of the same analysis. You have here gH.cgi, correct?

A Correct.
Q And that would be the file that the script will use if the QNAP was based on an IC86 architecture, correct?
A Correct.
Q When you were analyzing the script, you determine that this was a CGI factor, didn't you?
A Correct, I did.
Q And yesterday you say that this determination was wrong, turned out to be wrong.
A I believe that statement was wrong. I believe this was the CGI back door.
Q So, yesterday you testified that these notes were wrong and today you're testifying that these are actually right.
A They're wrong in parts. The earlier part was wrong. This part I believe is right.
Q So, what do you currently believe of armgH, is that an IRC bot or a back door?
A I believe armgH is the back door.
Q Okay. Is it true that armgH and gH contain binary language pointing to the 192 server which goes to ppolloo.org?
A I don't recall.
Q Okay. Let me refresh.
MR. BERTOLLINI: I actually left some of my notes there.
THE COURT: Please.

What if you get a new IP? What part of the IP address changes?
A The entire IP address may change.
Q The entire.
A Again, that depends on how your ISP configures the network.
Q Not just the last of the four, five or the last two, you're saying all of it.
A Not only the last part may change, but anything may change.
THE COURT: "ISP" means?
THE WITNESS: Internet service provider.
THE COURT: Okay.
Q So, you say often it changes only the final five, correct?
A Correct.
Q You mean the fourth of the four parts or the third and fourth parts?
A The third and fourth is very common.
Q Very common, correct?
A Correct.
Q Let's go back for a second to the CL file. How, if anything, is that related to clicks or click fraud?
A CL is not related to click fraud.
Q Yesterday, you also testified with respect to the user

A Yes, they do.
Q And mobile phone click-through rate?
A Mobile click-through rates are in the one to five percent range.
Q Meaning that every 100 visits on average is only two clicks, correct?
A Correct.
Q Does an advertiser need cookies to verify validity of a click?
A Yes, cookies are used as part of that.
Q Yesterday, you testified with respect to the EMME.
A Yes, I remember.
Q You testified that the script, when it runs, IT downloads the banners four times, correct?
A It attempts to download banners four times, I believe is what I said. The last version fails on QNAP devices, the last of the four times fail.
Q After the script downloads the banners, how many clicks, if any, does EMME?
A This should not trigger any clicks, it will just trigger exposures.
Q What you're saying, in other words, is that the EMME script only views the banner correct?
A Correct.
Q It does not click on the banner, correct?

correct?
A During a test of our maintenance system, yes.
Q .cgi?
A Correct.
Q So, let's assume we have a QNAP that does not have .cgi. Will that QNAP be infected or not infected?
A It would not be infected by this particular bot.
Q You just said from this particular version?
A Correct.
Q Because there are, in your opinion, different versions of this, correct?
A There are many different versions.
Q Many different versions.
Yesterday, you testified that you have not witnessed an operating IRC botnet of QNAP devices, correct?
A Correct.
Q If the QNAP device infected with the files do not connect with an IRC chat, what do they do?
A They just sit there and try to connect, but that's it.
Q They don't click, do they?
A They don't click.
MR. BERTOLLINI: Can I confer one moment, your Honor?
THE COURT: Yes, you may.
(Pause in proceedings.)

A So, I visited all these websites listed here. And for three of them, I found that they were QNAP NAS devices that were still connected to the internet and available.

MS. WELLS: I'd like to show the Court and the witness what is in evidence as Government Exhibit 12.

Q Mr. Cruz, take a look at Government Exhibit 12. Do you recognize that?

A Yes.

Q What is it?

A This is a screen shot of the browser that was used to navigate to this particular URL.

Q Let's take a look at the top section here. What website did you visit?

A IP address 217.133.67.226.

Q And does that same website IP address appear on 1332?

A Yes.

Q And where is that?

A It's the fifth line from the bottom.

Q Here?

A Yes.

Q Taking a look back at Government Exhibit 12, what is contained in this screen shot?

A That is the log-in page for a QNAP device.

Q How do you know it's a log-in page for a QNAP device?

A If you look at the top left corner, it identifies the

type of device.
Q What does it say?
A QNAP.
Q And how do you know it's a log-in page?
A If you look at the URL, the URL navigates to the login.html page.
Q And can you tell us where that's indicated?
A Following cgi-bin/login.html.

In addition to that, this interface shows an authentication panel that would prompt the user to use their user name and password to be able to log in to this device.

Q Where is that located on the screen shot?
A That is located in the center.
Q Here?
A Yes.
Q What are the empty fields?
A User name and password.
Q Mr. Cruz, by the way, who took this screen shot, Government Exhibit 12?
A I did.

MS. WELLS: I'd like to also show the witness what is in evidence as Government Exhibit 10.

THE COURT: All right.

Q Mr. Cruz, do you recognize Government Exhibit 10?
A Yes.

Q What is this?
A This is another screen shot of a navigation that I did to a specific URL that I found on the web log-ins artifact.
Q And when you say the web log-ins, are you referring to the exhibit here 1332?
A Yes.
Q In this instance, what location did you visit?
A A device with assigned IP address 213.127.210.232.
Q Is that IP address, 213.127.210.232, also listed as one of the web log-ins on Government Exhibit 1332?
A Yes.
Q And where is that located?
A The third item from the bottom.
Q There?
A Yes.
Q And, so, Mr. Cruz, when you visited this website, the 213 dot website, what did you find?
A Again, I found that this is the URL to a QNAP device.
Q How are you able to tell that it was a QNAP device?
A If you look at the bar on the left-hand corner, it identifies the type of device.
Q What does it say?
A QNAP.
Q And what kind of -- when you navigated to this location and went to the 213 IP address location, what kind of screen

is this?
A This is the log-in page.
Q And how can you tell?
A Again, if you look at the contents of the page, in addition to the login.html page that is referred to the URL and, also, see on the center of that user is prompted for entering user name and password to be able to log in.
Q And Mr. Cruz, did you visit any other websites listed here on 1332?
A Yes, I visited them all and I was able to view three of them.
Q So, let's take a look at what is in evidence as Government Exhibit 11. Do you recognize this, Mr. Cruz?
A Yes.
Q What is it?
A This is another screen shot of another navigation that I conducted.
Q And did you take the screen shot or did someone else?
A I did.
Q And from the file we just looked at a moment ago, Government Exhibit 10, who took that screen shot?
A I did.
Q So, what website or what URL did you visit here for Government 11?
A It's a device associated with IP address 203.45.155.11.

Q And is that location also listed on Government 1332 with web log-ins from hard drive six?
A Yes.
Q And where is that IP address listed?
A It's the fourth line from the bottom.
Q Can you read in that file name, please?
A Yes. That's http://203.45.155.11.
Q The remaining characters in that website, what are they?
A So, after the IP address --
Q Sorry, just read them.
A 8080cgi-bin.
Q Does that also match the content of the URL in Government Exhibit 11 on the right?
A Yes.
Q So Mr. Cruz, taking a look back at Government 11, what kind of screen are we looking at?
A The log-in page for QNAP device.
Q And once again, how are you able to tell it's a QNAP device?
A By looking at the screen, it identifies the name of the device in the top left-hand corner.
Q What does it say?
A QNAP QTS 4.1.0.
Q And what kind of screen is it?
A Again, it's a log-in page.

Q What is agent.php?
A agent.php is a PHP script that is designed to select from nine differ user agent strains at random.
[redacted]
BY MR. BERTOLLINI:
Q Is agent.php a malware?
A I don't know if it's specifically a malware, but I don't see -- there is -- there is either -- it's either software or malware. I don't see it -- it would have to be used in conjunction with something else.
Q You wrote a report in connection with this matter, correct?
A In reference to the analysis of the Linode server?
Q Correct.
A Yes, a report about that.
Q Isn't it true that in that report you wrote that agent.php is a simple PHP file?
A Yes.
Q What do you mean by simple?
A It contains only one function that is designed to choose from nine different user agent strains.
Q If someone has older browser, can the agent.php be used in that browser to navigate into websites?

actually work, did you?
A I didn't test it, no.
Q With respect to the 192 is related to the IRC.hold.org, have you analyzed the IRC domain?
A I don't understand the question. What do you mean by analyze the domain?
Q Have you navigated into the specific IP address?
A The irc.pollo.org domain or IP address?
Q Either one or both.
A No, I did not navigate to either one of those.
Q So you don't know who is the owner of pollo.org?
A I do not know.
Q You don't know who is the owner of 192 server associated with this domain?
A No.
Q Have you ever seen this particular botnet operated?
A Out in the wild, no.
Q Say that again, sorry.
A Out in the Internet, no.
Q So, you only saw it on paper.
A Yes.
Q Have you ever examined any of the IP addresses contained in the config.h file?
A What do you mean by examine?
Q Navigating to them?

A No.
Q Have you reviewed the content? I will rephrase.
Have you reviewed the image of any of those IP addresses, of those servers?
A The only image that I received was the image of the Linode server and the four other computers.
Q So the answer is no?
A No.
Q Talk about the masscan software, do you remember?
A Yes.
Q You also testified about QNAP devices out of the Internet where you navigated, correct?
A Yes.
Q Isn't it true that those QNAP devices were port 88?
A Yes.
Q Isn't it true that the masscan log that you found related to port 23?
A Yes.
Q How is the masscan log related to the QNAP?
A So, I testified and I annotated on my report, that I found these things. I did not attempt to relate these two-- particularly the QNAP case. I only testified that I found a log file that showed a scan session of specific IP addresses on port 23.
Q Did you find any evidence that the masscan was actually

files from specific directories.

Q Okay. So, what's the status of port 26 on your nmap analysis?

A Port 26, it's not shown.

Q Does that mean it's closed?

A Yes, it means it's closed.

Q You just testified that you examined the script existing in the malware that will attack the QNAP device, correct?

A Yes.

Q [redacted]

Q Do you know if any of these 12 IP addresses ever downloaded anything from the 178 server?

A No. I would have to check the access logs to actually see if there was any downloads.

Q You were also shown four separate QNAPs in evidence as Exhibit 9, 10, 11, and 12, remember?

A Yes.

Q Are you aware that none of these IP addresses associated with these QNAPs ever downloaded anything from the 178 server?

A No, not aware.

Q Did you check if they ever download anything?

A Yeah, I checked -- when I originally did this, I checked all these IP addresses that appear in the forensic image, and I recall that some of them did exist in the access logs.

Q Some of them? Which ones?

A I don't have a specific -- I don't have a list of the ones that did.

Q Do you know the owner of any of these four QNAP devices?

A No, not the owners, no.

Q Have you ever examined any of these four QNAP devices?

A "Examined" as in?
Q The physical device.
A Physical device or forensic image? No.
Q Have you tried to log into any of these device?
A No.
Q So, you didn't input the user name "request."
A Negative, no.
Q So you don't know if that would actually had worked, correct?
A Correct.
Q Now, you produced the list of IP addresses that downloaded agent.php from 178, right?
A Yes.
Q How would you determine if any of these IP addresses is a QNAP device?
A I didn't determine that.
Q Okay. So, they might not be QNAP devices?
A They might not be, no.
Q Did you find the actual IRC software on the 178 server?
A What do you mean by IRC software?
Q The software to run the chat.
A Can you repeat the question?
Q Did you find the software to run the IRC chat on that server?
A Yes, that is the lightaidra.

Q Isn't it true that you can use the software eraser.exe to protect your browser?
A Yes, that could be one of the reasons to use it, yes.
Q For example, will you be able to use it if you want to sell your hard drive?
A Yes.
Q Do you know if Fabio Gasperini invented the software lightaidra?
A No, I don't know that.
Q Isn't it true that lightaidra is an open source?
A Yes.
Q What does it mean?
A An open source tool is a piece of software that's openly available on the internet for anybody to be able to access it and use it.
Q Are you aware that none of those 12 IP addresses that you found as a reference in the hard drive are not American?
A I don't understand the last part of your question.
Q Are you aware that none of the 12 IP addresses are U.S. based?
A Yes, I am aware. I did look up the three or four that I was able to connect to and they were assigned to Italy and Australia.
MR. BERTOLLINI: No further questions, your Honor.
(Continued on next page.)

Q Was Dianele Gasperini in the home at the time that you conducted the search?
A Yes.
Q Did he say anything to you about what happened to the hard drives from the computers in 1207?
A Yes. We did ask why the computers had no hard drives and he replied by saying that they broke down and they were thrown away.
Q Aside from computers, did you seize anything else from the home that you were searching?
I'm sorry, let me be more specific. Did you seize any documents from the home?
A Yes.
Q Could you describe where the documents were?
A Some were in the bedroom. Some were in the entryway, in that hallway.
Q I am going to hand you what has been marked as Government Exhibit 1201. Open it. What is that, Mr. Pereno, just generally?
A It's a hard drive.
Q What does that hard drive contain?
A This hard drive has only copies of all the hard discs that were seized during the search.
Q Does it also have copies of the documents that were seized?

A They're not contained in this hard drive. They are in another hard drive.
Q So that hard drive contains forensic copies of hard drives that you obtained at Via Dei Frassini 132 in July 2016?
A Yes. The forensic copy of all the hard drives.
Q And does it contain a true and accurate copy of those things?
A Yes.
Q You have reviewed that disc before you came into court today?
A Yes.
Q Are there any markings on the exhibit that indicate that you have reviewed it?
A His signature and the date are on the hard drive.
MS. KOMATIREDDY: The Government moves Government Exhibit 1201 into evidence.
MR. BERTOLLINI: Objection, Your Honor. Lack of identification.
THE COURT: Did you want to voir dire the witness about it?
MR. BERTOLLINI: Yes, your Honor.
THE COURT: Well, go ahead.
VOIR DIRE EXAMINATION
BY MR. BERTOLLINI:
Q Mr. Pereno, did you review the content of the original

hard drives?

A He has done a general forensic review and done a general review of the hard drives but hasn't done it in detail.

MR. BERTOLLINI: I believe he said copy and not review in the first part.

THE COURT: Well, you are not the interpreter, so I go with the interpreter.

Next.

THE INTERPRETER: I'm sorry.

MR. BERTOLLINI: Okay, Your Honor, the witness has just testified he hasn't examine the content. He said that he had a cursory look at the hard drive. He can't testify as to the accuracy.

THE COURT: Anything else?

MS. KOMATIREDDY: I can add two more questions, Your Honor.

THE COURT: Go ahead.

DIRECT EXAMINATION

BY MS. KOMATIREDDY:

Q Did you do any forensic examination of what has been marked as Government Exhibit 1201 before coming into court today?

A Yes. Sorry. At the time it was seized, they have done a general examination of the hash contained in the hard drive and he matched the data from the hard drives to make sure that

it was in confirmatory with the original hard drive.
Q What is a hash?
A A hash is a string that is associated with what's contained in that file and the calculation determines that if two files that have been examined are matched -- if two hash are similar, it means that the two files that have been examined match, are the same.
Q Is it if two hashes are similar or if two hashes are the same?
A The same.
Q So if two hashes are the same, then the files are the same; is that right?
A Yes.
Q And the hash is a unique number that is associated with the file?
A Yes.
Q And is it fair to say a hash value is like a fingerprint for a file?
A Yes.
Q And when you first seized these hard copies and copied them on to Government Exhibit 1201, you observed the hash value of every file?
A Yes. They were matched and calculated at the time, right after the ceasing.
Q And before you came into court today, you looked again at

Government Exhibit 1201 and you saw it had the same hash value, the same fingerprint as the hard drives that you seized in Italy?

A Yes. He verified that the hash was the same and therefore the files are the same.

MS. KOMATIREDDY: The Government moves 1201 into evidence.

MR. BERTOLLINI: Objection, Your Honor. He relied on the software and the hash is only generated by the software.

THE COURT: The objection is overruled.

Government Exhibit 1201 is received in evidence.

(Government's Exhibit 1201 was received in evidence.)

Q Now, Mr. Pereno, you testified that there are copies of four hard drives on Government Exhibit 1201; correct?

A Yes.

Q You also testified that you recovered more than four hard drives or computers from the apartment. What was the state of the other hard drives?

A The other three hard drives were not functioning. They were broken, therefore, we couldn't exam their content.

(Continued on following page.)

Q As of today, have you or have you not reviewed the content of the hard drives you turned over to the U.S. Government?
A He hasn't done the search in depth. He verified that the copy had been done correctly.
Q Do you know what a QNAP device is?
THE INTERPRETER: Sorry, could you repeat.
Q Do you know what a QNAP device is?
A Yes.
Q Have you ever worked or examined any QNAP device?
MS. KOMATIREDDY: Objection. Scope.
THE COURT: Sustained.
Q Do you know anything about the Shellshock vulnerability?
MS. KOMATIREDDY: Objection.
THE COURT: Sustained.
Q You are a cybercrime expert; correct?
MS. KOMATIREDDY: Objection. We have not offered the witness as an expert.
THE COURT: Sustained.
Q Let me draw your attention to the first invoice I just showed you. Can you tell us what is the net amount paid -- no, billed in this invoice?
A The net import is 371 Euros and 25 Euro cents.
Q You previously testified that this relates to the amount of September 2014?

the ordinary course of business, correct?
A Yes, it is correct.
Q But earlier, you testified that you never worked for Leonardo ADV, correct?
A It is correct.
Q Do you have any evidence that the campaigns run by U.S. companies were ever assigned to any of Gasperini's websites?
A We don't have any evidence that for sure, this campaigns were run on Gasperini's websites.
Q Do you know under what categories of advertisement this campaigns belonged to U.S. companies, failed to--
A Depends on the type of advertiser, some of them are commercial, some are entertainment, some are charity.
MR. BERTOLLINI: Now, may I briefly confer?
THE COURT: Surely.
(Pause.)
(Transcript continues on next page.)