

**IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA**

**Alexandria Division**

UNITED STATES OF AMERICA

v.

DARRYL JULIUS POLO,  
a/k/a djppimp,

*Defendant.*

No. 1:19-CR-253-2

The Honorable T.S. Ellis, III

**STATEMENT OF FACTS**

The United States and the defendant, Darryl Julius Polo, a/k/a djppimp, agree that the allegations in the indictment and the following facts are true and correct, and that had this matter proceeded to trial, the United States would have proven the following facts beyond a reasonable doubt with admissible and credible evidence:

**A. The Defendant's Operation of iStreamItAll**

1. From at least 2014 to September 2019, the defendant owned and operated iStreamItAll (ISIA). Based in Las Vegas, Nevada, ISIA was a subscription-based service permitting the unlawful streaming and downloading of copyrighted works without the permission of the copyright owners. ISIA was accessible from various devices and platforms, including computer operating systems, smartphones, tablets, smart televisions, video game consoles, digital media players, set-top boxes, and web browsers.

2. ISIA had thousands of paid subscribers across the United States, including within the Eastern District of Virginia. For example, a partial list of ISIA subscribers for a 27-month period from September 4, 2014, through December 5, 2016, shows 18,551 successful credit and

debit card transactions by subscribers, which equates to ISIA receiving on average 22 subscriptions fee payments every day. Moreover, between May 9, 2017, and June 10, 2017, more than 20 individuals residing in the Eastern District of Virginia paid for subscriptions to ISIA, including E.S., a resident of Dumfries, Virginia; R.J., a resident of Centreville, Virginia; and B.W., a resident of Prince George, Virginia.

3. In operating ISIA, the defendant hired computer programmers through an online marketplace; used accounts in the name of his wife, L.P., or his defunct sport memorabilia and card company, Sincity Sports Cards; and willfully reproduced and made available to users of ISIA for streaming and downloading tens of thousands of copyrighted television episodes and movies without obtaining authorization from or paying the copyright owners.

4. In November 2017, the Federal Bureau of Investigation (FBI) executed a search warrant at a Las Vegas residence belonging to the defendant, seizing evidence relating to the defendant's criminal infringement of copyrighted works, including data on approximately 30 electronic devices. Nevertheless, the defendant continued to operate ISIA until September 2019, when the FBI seized two domains used by the service.

***Defendant's Sourcing and Hosting of Infringing Works***

5. ISIA made available to its subscribers more than 118,479 different television episodes and 10,980 individual movies, which was more content than that offered by Netflix, Hulu, Vudu, Amazon Prime, and other licensed streaming services. In fact, the defendant sent out emails to potential subscribers highlighting ISIA's huge catalog of works and urging them to cancel Netflix, Hulu, and similar services, and subscribe to ISIA instead.

6. The defendant used servers and computers in the United States and Canada to search for, download, process, store, stream, and make available for download infringing (or, “pirated”) television shows and movies.

7. The television shows and movies made available for streaming and downloading on ISIA were primarily sourced from torrent sites and Usenet NZB sites hosting pirated content. The defendant used automated software programs—such as SickRage, Sick Beard, and SABnzbd—to scour popular torrent and Usenet sites for pirated television shows and movies; download those works; and then process, store, and make those works available for streaming and download through ISIA. These tools allowed the defendant to search for pirated movies and television shows available on some of the most popular torrent sites in the world, such as The Pirate Bay, RARBG, and TorrentDay, as well as some of the largest Usenet NZB index sites, such as NZBplanet, NZBgeek, and NZB Finder. These software programs essentially operated 24 hours a day, 7 days a week.

8. On November 16, 2017, the FBI conducted a search of the defendant’s residence in Las Vegas. The search yielded copies of approximately 27,468 television episodes on various electronic devices located within the defendant’s residence, a small percentage of the total number of works available on ISIA that were stored on—and streamed and distributed from—the defendant’s rented servers in Canada.

#### ***ISIA Subscribers and Subscription Payments***

9. ISIA subscribers accessed the service’s infringing content through the Internet. For example, ISIA customers could go to ISIA by visiting the domains *istreamitall.com* or *istreamitall.mobi*. Likewise, they could access ISIA through smartphone applications (apps) available for download through various app sites; through a private channel on Roku, a set-top

streaming video player; and as an “add-on” for Kodi, an open-source media player software application. The defendant controlled the domains *istreamitall.com* and *istreamitall.mobi*, the ISIA smartphone apps, the ISIA private channel on Roku, and the ISIA Kodi add-on.

10. To join ISIA, users had to provide a debit or credit card and choose one of several subscription plans: a monthly option at \$19.99, a quarterly option at \$54.99, a semi-annual option at \$99.99, and a yearly option at \$179.99. A subscription payment typically would go through a payment gateway and then be executed by a payment processor. The payment gateway acted like an online point-of-sale terminal to authorize payments for card-not-present transactions and then transmit the online payment data to the payment processor. The payment processor, in turn, executed the transaction by transmitting the data between the merchant, the customer, the bank that issued the customer’s debit or credit card, and the bank that provided the merchant’s processing services. The defendant used numerous payment gateways and processors in his operation of ISIA, including Authorize.net, BankCard USA, EVO, Global Payments/North American Bancard, PayPal, PaySimple, and Stripe.

11. The subscription payments were sent to the defendant through the payment gateways and payment processors. The payment processors would make batch payments—that is, lumping multiple subscription payments together before transferring them—to a Wells Fargo bank account ending in 8077 that the defendant controlled. The defendant would then use the funds in this bank account, which was in L.P.’s name, to pay expenses for ISIA and his other piracy operations, which are discussed in more detail below.

***The Defendant's Other Piracy Services***

12. Besides ISIA, the defendant ran other piracy services and associated Internet domains. Since at least 2012, he operated SmackDownOnYou (SDOY), BoxBusters.TV, Jailbreakingtheipad, and MixtapeUG, which are described further below.

a. SDOY is a Usenet NZB indexer service that enabled users, for a fee, to search for and download copyrighted movies, television shows, and other files. The defendant also used SDOY to source infringing works for ISIA.

b. The defendant used servers associated with BoxBusters.TV and Jailbreakingtheipad to locate and download pirated content for ISIA.

c. MixtapeUG was a site that facilitated the streaming and downloading of music via the Internet, including copyrighted songs that were otherwise available through legitimate commercial distribution sources. MixtapeUG was also available as a smartphone app.

13. As with ISIA, the defendant used servers in Canada in connection with his operation of SDOY, BoxBusters.TV, Jailbreakingtheipad, and MixtapeUG.

***The Defendant's Earnings from His Piracy Operations and Money Laundering***

14. The defendant earned over \$1 million from his piracy operations. Moreover, he persisted in the reproduction and distribution of infringing content despite the repeated closure of the accounts he used for those operations. For example:

a. The defendant used a PayPal account ending in 0496 to process payments for SDOY and MixtapeUG, receiving payments through his email addresses paypal@jailbreakingtheipad.com, darrylpolo@gmail.com, and djp@mixtapeug.com. Between June 22, 2012 and August 16, 2013, that PayPal account received \$236,482.11. PayPal

subsequently shut down this account due to concerns that the defendant was engaged in copyright infringement.

b. The defendant used an EVO account ending in 0869/2995 to collect payments from ISIA and SDOY. This account, which was opened following the closure of the PayPal account ending in 0496, received \$984,241.01 between January 1, 2015, and December 3, 2018, most of which constituted proceeds from ISIA.

c. From August 28, 2013, to April 6, 2014, the defendant used a Stripe account for SDOY and MixtapeUG, receiving \$62,905. From December 1, 2016, to May 4, 2017, the defendant used BankCard USA, receiving about \$137,746.67, almost all of which was from ISIA. And, from May 8, 2017, to June 11, 2017, the defendant used another Stripe account, receiving \$20,085.13 for ISIA. Ultimately, Stripe and BankCard USA terminated all of these accounts.

d. The defendant used an Authorize.net account as a payment gateway for his payment processors, and it facilitated the processing of \$1,158,717.71 between December 1, 2016, and August 25, 2019, almost all of which was from ISIA.

15. The defendant admits that he used profits from ISIA to further its illegal operation, and in doing so he engaged in money laundering. For example, as set forth in Count 16, on June 2, 2017, the defendant knowingly conducted a financial transaction affecting interstate or foreign commerce by making a payment through the Wells Fargo account ending in 8077 (which was in the name of L.P.) to a company headquartered in Foster City, California, to provide payment gateway services for ISIA. That payment involved the proceeds of a specified unlawful activity, that is, criminal copyright infringement and conspiracy to commit criminal copyright infringement in the Eastern District of Virginia.

16. The defendant made this payment with the intent to promote the carrying on of the specified unlawful activity. He also made the payment knowing that the transaction was designed in whole or in part to conceal or disguise the nature, location, source, ownership, or control of the proceeds of that specified unlawful activity. Moreover, while conducting the financial transaction, the defendant knew that the property involved in the financial transaction represented the proceeds of that specified unlawful activity.

*The Defendant's Distribution and Streaming of Specific Works*

17. The defendant admits that, as set forth in Count 6, "Us" was a copyrighted motion picture that as of May 27, 2019, had not been made available in copies for sale to the general public in the United States in a format intended to permit viewing outside a movie theater. In this regard, "Us" was a work being prepared for commercial distribution in the United States.

18. On or before May 27, 2019, the defendant willfully, and for purposes of commercial advantage and private financial gain, made "Us" available on ISIA. And, at least on May 27, 2019, the defendant distributed this work to the Eastern District of Virginia. Moreover, the defendant knew or should have known that "Us" was intended for commercial distribution at that time, that is, he knew or should have known that the work was not available then for authorized release in the United States through digital download, DVD, or Blu-ray.

19. The defendant further admits that, as set forth in Count 8, on January 4, 2017, he willfully, and for purposes of commercial advantage and private financial gain, infringed a copyright in the episode "Red on Red" of the television program "Shooter" by distributing a copy over the Internet to the Eastern District of Virginia.

20. The defendant also admits that, as set forth in Count 11, on December 29, 2016, he willfully, and for purposes of commercial advantage and private financial gain, infringed a

copyright in the motion picture “Inferno” by streaming—that is, publicly performing the work—over the Internet to the Eastern District of Virginia.

**B. The Defendant’s Involvement in the Operation of Jetflicks**

21. Before establishing ISIA, the defendant worked with co-defendant Kristopher Lee Dallmann and others to run Jetflicks, a service similar to ISIA. Jetflicks was headquartered in Las Vegas, Nevada, and was owned and operated by Dallmann.

***Background on Jetflicks and the Jetflicks Conspiracy***

22. Like ISIA, Jetflicks was an online, subscription-based service that permitted users to stream (and, at times, to download) copyrighted works despite lacking permission from the relevant copyright owners to do so. Jetflicks was accessible from a variety of devices and platforms, including computer operating systems, smartphones, tablets, smart televisions, video game consoles, digital media players, set-top boxes, and web browsers. The main difference between Jetflicks and ISIA was that Jetflicks offered only television shows.

23. At Jetflicks, Dallmann, the defendant, and others willfully reproduced tens of thousands of copyrighted television episodes, without the permission of copyright owners, and streamed and distributed the infringing programs to tens of thousands of paid subscribers located throughout the United States, including many individuals located within the Eastern District of Virginia.

24. Jetflicks could be reached through Internet-connected devices at the domain *jetflicks.mobi*. Jetflicks also used the domains *jetflicks.net* and *jetflicks.com*. In addition, Jetflicks could be accessed through mobile apps and a private Roku channel. Dallmann controlled the domains *jetflicks.mobi*, *jetflicks.net*, and *jetflicks.com*, the Jetflicks mobile apps,



and the private Roku channel, and he provided administrator and developer access to the domains, the apps, and private channel to others at Jetflicks, including the defendant.

25. Similar to ISIA, Jetflicks obtained television shows from sites hosting infringing content (such as torrent sites and Usenet NZB sites), and used automated programs and databases (such as SickRage, Sick Beard, SABnzbd, and TheTVDB) to do so. Dallmann, the defendant, and others at Jetflicks used servers and computers in the United States and Canada to search for, download, process, store, stream, and make available for download infringing television programs.

26. To become a user of Jetflicks, customers visited *jetflicks.mobi* through an Internet-connected device and then used a debit or credit card to purchase a subscription. The subscription payments typically would go through a payment gateway and then be executed by a payment processor. As with ISIA, the relevant payment processor often would batch subscription payments, depositing them in a lump sum in a bank account controlled by Dallmann.

27. The defendant admits, as set forth in Count 1, that starting around May 2012 and continuing through around July 2016, Dallmann, co-defendant Douglas Courson, co-defendant Felipe Garcia, co-defendant Peter Huber, the defendant, and others at Jetflicks knowingly and intentionally conspired and agreed to willfully and for purposes of commercial advantage and private financial gain infringe copyrights by reproduction and distribution of at least ten copies of one or more copyrighted works without permission from the right holders during a 180-day period with a total retail value of more than \$2,500.

28. The defendant also admits that at least the following subscriptions in the Eastern District of Virginia occurred during the course of the conspiracy alleged in Count 1:

a. On July 24, 2012, \$29.99 was charged to a Visa card number ending in 2153, which belonged to M.T., a resident of Ashburn, Virginia, for a six-month Jetflicks subscription;

b. On March 9, 2016, \$133.75 was charged to a Visa card number ending in 7270, which belonged to L.S., a resident of Arlington, Virginia, for an annual Jetflicks subscription with additional services.

c. On February 24, 2016 and May 24, 2016, \$19.99 was charged to a Visa card ending in 3600, which belonged to B.P., a resident of Alexandria, Virginia, for a three-month Jetflicks subscription.

d. On April 15, 2016, \$19.99 was charged to a Visa card ending in 1030, which belonged to S.M., a resident of Alexandria, Virginia, for a three-month Jetflicks subscription.

29. The defendant and his co-conspirators knew that Jetflicks was engaged in copyright infringement. For example, Jetflicks was blocked from using certain applications and services due to concerns of copyright infringement, but the conspirators continued to operate and expand Jetflicks. Likewise, on November 16, 2012, Dallmann received from the Motion Picture Association of America (MPAA), on behalf of its members, cease-and-desist letters that were sent by hand delivery, Federal Express, and email. The letters demanded that Jetflicks discontinue its unauthorized distribution of copyrighted material. A few days later, the defendant searched the internet for “mpaa website moles,” “fake mpaa user account,” “correct letter to dmca response,” and “dmca reply,” and visited various related sites, including an article entitled “MPAA / RIAA Want U.S. to Help Quash The Pirate Bay.”

*Defendant's Role at Jetflicks from May 2012 to September 2013*

30. Individuals at Jetflicks performed various roles, and sometime multiple roles, that served to promote the success of the conspiracy. Some of the roles included management; computer programming and coding; design of website, apps, and customer interface, and technical assistance; subscriptions and revenue; and customer support.

31. From around May 2012 to September 2013, the defendant worked at Jetflicks with Dallmann, Courson, Garcia, Huber, and others. During this period, the defendant wrote computer code for and helped develop the Jetflicks Android smartphone app; provided advice regarding improving Jetflicks' search engine and app rankings, increasing Internet and mobile traffic to Jetflicks, boosting the number of customers, and advertising and distributing the Jetflicks app (including advertising Jetflicks on sites that the defendant ran, such as SDOY and DapperCell); helped find pirated television shows for Jetflicks through SickRage, Sick Beard, Usenet NZB indexer sites (including the defendant's own SDOY), and otherwise on the Internet, downloaded those works, and assisted in providing them to customers to watch or download; offered Dallmann a security tool to prevent others from "steal[ing] [his] files"; helped select and download popular television shows based on feedback from customers; provided assistance regarding the quality of television shows uploaded to the Jetflicks library and how to repair them; and offered aid with regard to cleaning up the text and display of shows in the Jetflicks library. From around June 4, 2012 to September 19, 2013, Dallmann paid the defendant at least \$85,300 for his contributions to Jetflicks.

32. Dallmann played numerous roles at Jetflicks including running the Jetflicks operation; coding and writing computer programs and scripts; designing the Jetflicks website, apps, and customer interface and providing technical assistance; working to increase

subscriptions and revenue; and supervising and providing customer support. Dallmann was involved in every significant aspect of managing Jetflicks.

33. Courson also had many responsibilities with Jetflicks. For example, Courson worked with Sick Beard and SickRage to download and process infringing content such as television programs requested by customers and new or upcoming shows; helped design the Jetflicks interface; monitored the load of Jetflicks' servers and helped ensure the functioning of the servers; kept track of Jetflicks' actual and projected revenue and subscriptions, and worked on ideas to increase profitability and encourage subscriber renewals; assisted with customer support; and aided management of the operation, including helping to hire Garcia.

34. Garcia handled customer support. Based on customer feedback, he would flag customer requests for television programs, report missing/broken shows, and suggest downloading upcoming shows to Courson and others, who could then obtain them through Sick Beard or SickRage. Garcia also suggested changes to the Jetflicks interface.

35. Huber did computer programming and coding for both the Jetflicks app and website; was involved in downloading and uploading television programs; handled processing issues involving broken shows; worked on the Jetflicks interface including design, as well as functionality for subscribers; monitored use of Jetflicks servers; and assisted Dallmann with choosing hardware for Jetflicks.

***Defendant's Role at Jetflicks from December 2015 to July 2016***

36. After leaving Jetflicks in September 2013, the defendant returned to Jetflicks from around December 2015 through July 2016, working with Dallmann, Courson, and others.

37. Again, the defendant provided computer programming and coding expertise for Jetflicks. He also responded to complaints about broken shows, requests for new shows, billing

issues, questions about customer accounts, reports about system problems, and queries about how to use Jetflixs on devices such as Roku or Xbox. During this time, the defendant received an email from a member of the conspiracy using the email address support@jetflixs.com stating, “You are a vital team member... we are a team” and discussing plans for a “massive” project to increase the number of television programs at Jetflixs, enhance the quality of the new uploaded shows and avoid customer complaints, and improve the ways the television programs displayed in Jetflixs. For approximately six months of work in 2016, Dallmann paid the defendant \$20,500.

38. During this time, the defendant copied and retained numerous files pertaining to Jetflixs. For example, he kept a copy of a Jetflixs customer transaction list that showed 7,142 successful subscription transactions by individuals around the United States to Jetflixs in a five-month period from February 9, 2016 through July 7, 2016, which equates to an average of over 47 subscriptions each day. Over 100 of these transactions came from subscribers in Virginia, many of whom were in the Eastern District of Virginia.

39. The actions taken by the defendant, as described above, were all taken willfully, intentionally, and knowingly. The defendant did not take those actions by accident, mistake, or with the belief that they did not violate the law.


40. The defendant admits that the infringement amount for his offenses is more than \$250,000 and no greater than \$550,000; that the offenses involved the display, performance, publication, reproduction, or distribution of a work being prepared for commercial distribution; and that the offenses involved the manufacture, importation, or uploading of infringing items.

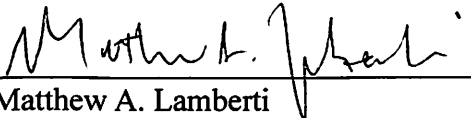
41. This statement of facts includes those facts necessary to support the plea agreement between the defendant and the United States. It does not include each and every fact

known to the defendant or to the United States, and is not intended to be a full enumeration of all the facts surrounding the defendant's case.

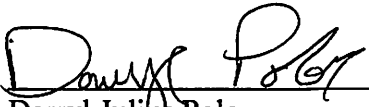
Respectfully submitted,

G. Zachary Terwilliger  
United States Attorney

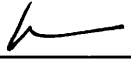
By:   
Alexander P. Berrang  
Assistant United States Attorney

  
Matthew A. Lamberti  
Senior Counsel, U.S. Department of Justice

Defendant's Signature: After consulting with my attorney and pursuant to the plea agreement entered into this day between the United States and me, I hereby stipulate that the above Statement of Facts is true and accurate, and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.

Date: 12-10-19   
Darryl Julius Polo  
Defendant

Defense Counsel Signature: I am counsel for Darryl Polo. I have carefully reviewed the above Statement of Facts with him. To my knowledge, his decision to stipulate to these facts is an informed and voluntary one.

Date: 12-10-19   
Elizabeth Mullin, Esq.  
Counsel for the Defendant