UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
- - - - - - - - - - - - - - - - - - -x

UNITED STATES OF AMERICA	:	**INDICTMENT**
- v. -	:	S1 12 Cr. 185 (LAP)
RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary" DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," DONNCHA O'CEARRBHAIL, a/k/a "palladium," and JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," a/k/a "ghost" a/k/a "anarchacker,"	:	
Defendants.	:	

- - - - - - - - - - - - - - - - - - -x

COUNT ONE

(CONSPIRACY TO COMMIT COMPUTER HACKING - INTERNET FEDS)

The Grand Jury charges:

THE DEFENDANTS

1. At certain times relevant to this Indictment, RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," and

JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," the defendants, were computer hackers who resided in the United Kingdom.

2. The role of RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," the defendant, included, among other things, identifying and exploiting vulnerabilities in victims' computer systems for the purpose of gaining unauthorized access to those systems for the groups charged in Counts One and Two of this Indictment.

3. The role of JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," the defendant, included, among other things, acting as a spokesman for the groups charged in Counts One and Two of this Indictment, for example by engaging in interviews with the media and publicizing those groups' hacking activities; drafting press releases; and organizing and storing confidential information stolen in connection with the computer hacking described in Counts One and Two of this Indictment.

4. At certain times relevant to this Indictment, DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," and DONNCHA O'CEARRBHAIL, a/k/a "palladium," the defendants, were computer hackers who resided in Ireland.

5. At certain times relevant to this Indictment, JEREMY HAMMOND, a/k/a Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," a/k/a "ghost," a/k/a "anarchacker," the

defendant, was a computer hacker who resided in Chicago, Illinois.

BACKGROUND ON ANONYMOUS AND INTERNET FEDS

6. Since at least in or about 2008, up through and including at least in or about March 2012, "Anonymous" has been a loose confederation of computer hackers and others sharing, among other things, common interests, common slogans, and common identifying symbols. During that time period, certain members of Anonymous have waged a deliberate campaign of online destruction, intimidation, and criminality, as part of which they have carried out cyber attacks against businesses and government entities in the United States and throughout the world.

7. Between in or about December 2010 and in or about May 2011, one group of individuals affiliated with Anonymous who engaged in such criminal conduct was composed of elite computer hackers who collectively referred to themselves as "Internet Feds." At various times relevant to this Indictment, members of Internet Feds carried out a series of cyber attacks against the websites and computer systems of certain business and government entities in the United States and around the world, including, among others, the following businesses and organizations:

a. Fine Gael, a political party in Ireland, which maintained the website "www.finegael2011.com;"

b. HBGary, Inc. and its affiliate, HBGary Federal, LLC (collectively referred to herein as "HBGary"), computer security firms based in the United States which provided computer security software and services, among other things, to their clients, and which maintained the website "www.HBGaryFederal.com;" and

c. Fox Broadcasting Company ("Fox"), a commercial broadcast television network in the United States, which maintained the website "www.fox.com."

8. These cyber attacks involved, among other things: (1) breaking into computer systems, deleting data, and stealing confidential information, including encrypted and unencrypted sensitive personal information for thousands of individual victims; (2) de-encrypting confidential information stolen from victims' computer systems, including encrypted passwords; (3) publicly disclosing that stolen confidential information on the Internet by dumping it on certain websites; (4) hijacking victims' email and Twitter accounts; (5) defacing victims' Internet websites; and/or (6) "doxing," that is, publicly disclosing online a victim's personal identifying information, such as the victim's name, address, Social Security number, email account, and telephone number, with the object of, among other things, intimidating the victim and subjecting the victim to harassment.

9. At various times relevant to this Indictment, and as part of Anonymous, members of Internet Feds sought to publicize their Internet assaults and intimidate their victims by, among other things: (1) posting messages online in which they discussed their attacks and threatened additional attacks; (2) using particular logos and slogans when, for example, they posted messages online and defaced websites; and (3) discussing their attacks with members of the press.

10. At various times relevant to this Indictment, and much like other members of Anonymous, members of Internet Feds, despite their efforts to publicize their illegal conduct, typically attempted to hide their true identities by, for example, using aliases when they communicated with the public or with each other.

11. At various times relevant to this Indictment, members of Internet Feds, much like other members of Anonymous, communicated using, among other means, Internet Relay Chat ("IRC") channels -- that is, real-time, text-based online forums. Some of these channels were open to the public. Others, particularly channels in which members of Anonymous and members of Internet Feds planned and organized criminal activity, including cyber attacks, were not. Instead, those channels were generally password-restricted and available by invitation only, usually to trusted individuals who had proven

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.