UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA **v.** **AARON SWARTZ,** **Defendant**	**Crim. No. 11-CR-10260-NMG** **VIOLATIONS:** **18 U.S.C. § 1343 (Wire Fraud)** **18 U.S.C. § 1030(a)(4),(b) (Computer Fraud)** **18 U.S.C. § 1030(a)(2), (b), (c)(2)(B)(iii) (Unlawfully Obtaining Information from a Protected Computer)** **18 U.S.C. § 1030(a)(5)(B), (c)(4)(A)(i)(I),(VI) (Recklessly Damaging a Protected Computer)** **18 U.S.C. § 2 (Aiding and Abetting)** **18 U.S.C. § 981(a)(1)(C), 28 U.S.C. § 2461(c), 18 U.S.C. § 982(a)(2)(B), and 18 U.S.C. § 1030(i) (Criminal Forfeiture)**

SUPERSEDING INDICTMENT

The Grand Jury charges that at all relevant times:

PARTIES

JSTOR

1. JSTOR, founded in 1995, was and continued to be a United States-based, not-for-profit organization that provides an online system for archiving and providing access to academic journals and journal articles. It provides searchable digitized copies of articles from over 1,000 academic journals, dating back for lengthy periods of time.

2. JSTOR's service is important to research institutions and universities because it can be extraordinarily expensive, in terms of both cost and space, for a research or university library to maintain a comprehensive collection of academic journals. By digitizing extensive, historical collections of journals, JSTOR enables libraries to outsource the journals' storage, ensures their preservation, and enables authorized users to conduct full-text, cross-disciplinary

searches of them. JSTOR has invested millions of dollars in obtaining and digitizing the journal articles that it makes available as part of its service.

3. JSTOR generally charges libraries, universities, and publishers a subscription fee for access to JSTOR's digitized journals. For a large research university, this annual subscription fee for JSTOR's various collections of content can cost more than $50,000. Portions of the subscription fees are shared with the journal publishers who hold the original copyrights. In addition, JSTOR makes some articles available for individual purchase.

4. JSTOR authorizes users to download a limited number of journal articles at a time. Before being given access to JSTOR's digital archive, each user must agree and acknowledge that they cannot download or export content from JSTOR'S computer servers with automated computer programs such as web robots, spiders, and scrapers. JSTOR also uses computerized measures to prevent users from downloading an unauthorized number of articles using automated techniques.

MIT

5. The Massachusetts Institute of Technology ("MIT") was and continued to be a leading research and teaching university located in Cambridge, Massachusetts.

6. JSTOR provided MIT with its services and content for a fee.

7. MIT made JSTOR's services and content available to its students, faculty, and employees. MIT also allowed guests of the Institute to have the same access to JSTOR, but required guests to register on the MIT network. MIT authorized guests to use its network for no more than fourteen days per year, and required all users to use the network to support MIT's research, education, and administrative activities, or at least to not interfere with these activities; to maintain the system's security and conform to applicable laws, including copyright laws; and to conform with rules imposed by any networks to which users connected through MIT's system. These rules explicitly notified users that violations could lead to state or federal prosecution. Guest users of the MIT network agreed to be bound by the same rules that applied to students,

faculty, and employees.

8. JSTOR's computers were located outside the Commonwealth of Massachusetts, and thus any communications between JSTOR's computers and MIT's computers crossed state boundaries. JSTOR's and MIT's computers were also used in and affected interstate and foreign commerce.

Aaron Swartz

9. Aaron Swartz lived in the District of Massachusetts and was a fellow at Harvard University's Safra Center for Ethics. Swartz was not affiliated with MIT as a student, faculty member, or employee or in any other manner. Although Harvard provided Swartz access to JSTOR's services and archive as needed for his research, Swartz used MIT's computer networks to steal millions of articles from JSTOR.

OVERVIEW OF THE OFFENSES

10. Between September 24, 2010, and January 6, 2011, Swartz contrived to:

a. break into a restricted-access computer wiring closet at MIT;

b. access MIT's network without authorization from a switch within that closet;

c. access JSTOR's archive of digitized journal articles through MIT's computer network;

d. use this access to download a substantial portion of JSTOR's total archive onto his computers and computer hard drives;

e. avoid MIT's and JSTOR's efforts to prevent this massive copying, efforts that were directed at users generally and at Swartz's illicit conduct specifically; and

f. elude detection and identification.

MEANS OF COMMITTING THE OFFENSES

11. Swartz alone, or in knowing concert with others unknown to the Grand Jury, (hereafter simply "Swartz" in this section) committed these offenses through the means described below.

September 24 through 27, 2010

12. On September 24, 2010, Swartz purchased an Acer laptop computer from a local computer store.

13. Later that day, Swartz connected the Acer laptop to MIT's computer network from a location in Building 16 at MIT and registered with MIT's computer network as a guest.

14. When Swartz registered on the network, he took measures to hide his identity as the computer's owner and user:

a. Swartz registered the computer under the fictitious guest name "Gary Host."

b. Swartz specified the computer's client name as "ghost laptop." (A computer's client name helps to identify it on a network and can be chosen by its user.) In this case, the "ghost" client name abridged the pseudonym "Gary Host" by combining the first initial "g" with the last name "host."

c. Swartz identified the fictitious "Gary Host's" e-mail address as "ghost@mailinator.com", a temporary e-mail address. Mailinator advertised itself as a free e-mail service that allows a user to create a new temporary-mail address as needed. Mailinator advertised that it would accept mail for any e-mail address directed to the mailinator.com domain without need for a prior registration or account. Mailinator also advertised that all mail sent to mailinator.com would automatically be deleted after several hours, whether read or not, and that the company kept no logs of e-mail access.

15. On September 25, 2010, Swartz used the Acer laptop to systematically access and

rapidly download an extraordinary volume of articles from JSTOR by submitting download requests faster than a human could type, and in a manner designed to sidestep or confuse JSTOR's computerized efforts to restrict the volume of individual users' downloads.

16. The effect of these rapid and massive downloads and download requests was to impair computers used by JSTOR to provide articles to client research institutions.

17. As JSTOR, and then MIT, became aware of these events, each took steps to block communications to and from Swartz's computer. Swartz, in turn, altered the apparent source of his automated demands to sidestep or circumvent JSTOR's and MIT's blocks against his computer, as described below:

a. On the evening of September 25, 2010, JSTOR terminated Swartz's computer's network access by refusing communications from the computer's assigned IP address.

i. An IP (short for "Internet Protocol") address is a unique numeric address assigned to each computer connected to the Internet so that the computer's incoming and outgoing Internet traffic is directed to the proper destination. Most Internet service providers control a range of IP addresses. MIT controls all IP addresses that begin with the number 18.

ii. Swartz's computer had been assigned an IP address of 18.55.6.215.

iii. On September 25, 2010, JSTOR blocked communications from that IP address, thus preventing Swartz from requesting and receiving any more JSTOR articles.

b. On September 26, 2010, Swartz established a new IP address for his computer on the MIT network – 18.55.6.216 – which sidestepped the IP address block and allowed the laptop to resume downloading an extraordinary volume of articles from JSTOR. Accesses from this address continued until the middle of the day, when JSTOR spotted the access and blocked communications from this

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.