**From: http://www.volokh.com/2013/01/14/aaron-swartz-charges/**

# The Criminal Charges Against Aaron Swartz (Part 1: The Law)

By **Orin Kerr** on January 14, 2013 2:50 am in **Computer Crime Law**, **Computer Fraud and Abuse Act**

The Internet activist Aaron Swartz has died from an apparent suicide. Swartz was facing a criminal trial in April on charges arising from his effort to "liberate" the JSTOR database, and there has been a lot of commentary accusing the prosecutors in his case of having abused their role in ways that contributed to Swartz's tragic death. Swartz's friend Larry Lessig led the way by angrily condemning the prosecutors who charged Swartz as "bullies" who acted like they "had caught the 9/11 terrorists red-handed." According to Lessig, the prosecutors acted in an "the most absurd or extreme way" and "don't deserve to have the power of the United States government." A lot of people seem to agree, and today's media has picked up the story. *The New York Times* is running a headline, "A Data Crusader, a Defendant and Now, a Cause." *The Associated Press* has a somewhat similar story, "Swartz' Death Fuels Debate Over Computer Crime".

The criticisms of the Swartz prosecution concern two different questions. The first question is the law. Were the charges against Swartz based on a fair reading of the laws? Or was the prosecution being overly aggressive or relying on strained theories in charging Swartz as it did? The second question is discretion and judgment. The DOJ has the discretion to charge cases or not, and prosecutors can agree to different plea deals or even agree to have charges dismissed. Were the prosecutors in this case unfair in how they exercised discretion, or did they act irresponsibly in the case in how they exercised the discretion that the law grants them?

I hope to answer these questions in two posts. In the first post, I'm going to try and answer the first question — the law — as informed by my background as a specialist in this particular area of law who has testified on these statutes before Congress, defended computer crime cases involving these statutes, and helped prosecute them, too. In a subsequent post, I'll try to answer the second question, the exercise of prosecutorial discretion.

This is going to be a long post, so here's the summary of my conclusion on the first question: I think the charges against Swartz were based on a fair reading of the law. None of the charges involved aggressive readings of the law or any apparent prosecutorial overreach. All of the charges were based on established caselaw. Indeed, once the decision to charge the case had been made, the charges brought here were pretty much what any good federal prosecutor would have charged. This is different from what a lot of people are hearing on the Internets, so I realize this post isn't going to be popular. But I'll explain my position in some detail, starting with the facts and then turning to the law, and then I'll open it up for comments. And in a subsequent post, I'll take on the second question of whether prosecutors properly exercised their discretion in the decision to charge the case and during plea negotiations.

*I. The Facts Alleged in the Indictment*

Here's the indictment filed in Swartz' case. Based on the indictment and news coverage of the case, the following is my current understanding of the facts:

JSTOR is an organization that sells universities, libraries, and publishers access to a database of over 1,000 academic journals. For a large research university, JSTOR charges as much as $50,000 a year for an annual subscription fee, at least parts of which go to pay copyright fees to the owners of the articles in the databases. The JSTOR database is not freely available: Normally, a username and password are required to access it. But if you access the site from a computer network owned by a university that has purchased a subscription, you can access the site without a username and password from their network. Users of the service then have to agree to use JSTOR in a particular way when they log in to the site; they generally can download one article at a time, but the JSTOR software is configured to block efforts to download large groups of articles.

Aaron Swartz decided to "liberate" the entire JSTOR database. He wanted everyone to have access to all of the journals in the database, so he came up with a plan to gain access to the database and copy it so he could make it publicly available to everyone via filesharing networks. Swartz lived in the Boston area, and he had legitimate access to the JSTOR database using Harvard's network, where he was a fellow. But Swartz decided not to use Harvard's network for what he had planned.

Instead, he used MIT's network across town. Swartz did not have an account or formal relationship with MIT, but MIT is known for having relatively open account practices.

In Swartz' first attempt, he purchased a laptop, went into a building at MIT, and used the MIT wireless network to create a guest account on MIT's network. He then accessed JSTOR and executed a program called "keepgrabbing" that circumvented JSTOR's limits on how many articles a person could download — thus enabling Swartz to start to download a massive number of articles. MIT and JSTOR eventually caught on to what was happening, and they blocked Swartz's computer from being able to access the MIT network by banning the IP address that he had been assigned.

Swartz responded by changing his IP address, and it took a few hours before JSTOR noticed and blocked his new IP address. To try to stop Swartz from just changing IP addresses again, JSTOR then blocked a range of IP addresses from MIT and contacted MIT for more help. MIT responded by canceling the new account and blocking Swartz' computer from accessing the MIT address by banning his MAC address, a unique identifier associated with his laptop.

Undeterred, Swartz tried again. This time he brought a new laptop and also spoofed the MAC address from his old one to circumvent the ban. Using the two laptops and the program designed to circumvent JSTOR's limits on downloading articles, he started to download a significant chunk of JSTOR's database. A day or two later, JSTOR responded by blocking all of MIT's access to JSTOR for a few days.

Again undeterred, Swartz came up with a different plan. Instead of trying to connect to the MIT network wirelessly, Swartz broke into a closet in the basement of a building at MIT and connected his computer directly to the network — hiding his computer under a box so no one would see it. Over a month or two period, he succeeded in downloading a major portion of JSTOR's database.

Investigators were on to Swartz at this point, however. They installed a video camera in the closet to catch Swartz when he accessed the closet to swap out storage devices or retrieve his computer. Swartz was caught on camera, and he even seems to have realized that he was being filmed; at one point he was filmed entering the closet using his bicycle helmet as a mask to avoid being identified. (Here's the picture.) Swartz was spotted on MIT's campus soon after by the police and tried to run away, but he was then caught and arrested. Federal charges followed.

*II. The Legal Charges Brought Against Swartz*

The indictment against Swartz alleged several different crimes. A bunch of the crimes overlap, but that doesn't mean that they are really treated separately: At sentencing the general practice is to take the most serious of the crimes as the basis for the sentence and to mostly ignore the rest. But the ordinary practice is to charge all the possible offenses committed in the indictment, even if they overlap, and then let the jury sort them out at trial or else drop some of the charges in a plea deal. Here are the different offenses charged, with a legal analysis of each.

(a) *Wire Fraud.* The Wire Fraud statute, 18 U.S.C. 1343, prohibits a scheme to gain "property" by false pretenses. This strikes me as a pretty strong charge here. The false pretenses are provided by the false identification and spoofing of Swartz' IP address and MAC address. Swartz was trying to trick JSTOR into giving him access to their database after they had specifically tried their best to ban him from doing so. And the "property" was the contents of the JSTOR database itself. Some might argue that the contents of the JSTOR database should not be considered "property." But I think that's a hard argument to make in light of *United States v. Seidlitz*, 589 F.2d 152 (4th Cir. 1978). In *Seiditz*, a former employee of a company named OSI used the username and password of another employee of the company to login and try to download a text-editing program named WYLBUR used for business applications. Seidlitz argued that the program was not "property" because the WYLBUR program was widely used by different companies. But the court disagreed:

Even though software systems similar to OSI's WYLBUR were in use at non-OSI facilities, the evidence that OSI invested substantial sums to modify the system to suit its peculiar needs, that OSI enjoyed a multi-million dollar competitive advantage because of WYLBUR, and that OSI took steps to prevent persons other than clients and employees from using the system permitted a finding that the pilfered data was the property of OSI and not, as the defendant contends, property in the public domain subject to appropriation by persons such as himself.

That reasoning seems to apply reasonably well to the JSTOR database, too. See also Carpenter v. United States, 484 U.S. 19 (1987) (recognizing a property right for purposes of federal fraud statutes for a business in confidentiality and use of information to appear in a forthcoming publication). It's possible to argue that *Seidlitz* is distinguishable, but I think it's an uphill battle.

(b) *Computer Fraud.* The next charges were brought under the Computer Fraud statute, 18 U.S.C. 1030(a)(4), which is a close cousin of the Wire Fraud statute. The two are usually charged together in computer crime cases, and there isn't really all that much that separates them that we need to dwell on here. So let's move on to the next crime.

(c) *Unauthorized Access.* The next charge was unauthorized access to a computer to obtain information valued more than $5,000, in violation of 18 U.S.C. 1030(a)(2)(C) and 18 U.S.C. 1030(c)(2)(B)(iii). I think this charge was a fair one. There are two notable legal issues here. First, was the information valued at more than $5,000? The answer is clearly yes under the leading case of *United States v. Batti*, 631 F.3d 371 (6th Cir. 2011). *Batti* dealt with the $5,000 requirement in the context of a video that was difficult to value. The Sixth Circuit concluded that the $5,000 refers to the value of the information obtained, not any loss or harm to the alleged victim in the case. Further, the court authorized the following methodology when "information obtained by a violation of § 1030(c)(2)(B)(iii) does not have a readily ascertainable market value." In such cases, the court held, "it is reasonable to use the cost of production as a means to determine the value of the information obtained." Creating thousands of journals over many years obviously costs more than $5,000, so that element is easily satisfied.

The second issue is whether Swartz exceeded authorized access to the JSTOR computer. As regular readers know, I have been fighting overly broad readings of "unauthorized access" for well over a decade as a scholar, defense attorney, and op-ed writer. But I think it's pretty clear that Swartz exceeded his authorized access here. JSTOR has a password-protected database that Swartz was trying to copy by circumventing code-based barriers to large-scale access, and Swartz was playing a cat-and-mouse game in which he kept trying to gain access to the database and JSTOR kept trying to block him. They blocked his IP address; he changed it. They blocked his MAC address; he spoofed it. They blocked access and he broke into a restricted closet and connected directly to MIT's network. This is not merely a case of breaching a written policy. Rather, this is a case of circumventing code-based restrictions by circumventing identification restrictions. I don't see how that is particularly different from using someone else's password, which is the quintessential access without authorization. So I think unauthorized access is established here, too.

(d) *Computer Damage.* The final charge brought was exceeding authorized access and thereby impairing the availability or integrity of information in ways that cause more than $5,000 or loss or involve more than 10 computers, in violation of 18 U.S.C. 1030(a)(5)(B) and 1030(c)(4)(A)(i)(I) & (VI). This is a plausible charge, although we'd need to know more details about the case to know if it is fully merited. I've already covered the elements of authorized access, so we can adopt that analysis above here and move on to the other elements.

To get to $5,000 in a 1030(a)(5) case, the easiest and most widely-accepted methodology in the caselaw is to focus on the time spent responding to the unauthorized access. Courts would generally just consider the hours spent by MIT and JSTOR in responding to Swartz and multiply those hours to get to an overall dollar figure. *See, e.g.*, *United States v. Middleton*, 231 F.3d 1207 (9th Cir. 2000); *United States v. Millot*, 433 F.3d 1057 (8th Cir. 2006). It sounds like MIT and JSTOR spent a lot of dealing with Swartz. If so, the time alone should pretty quickly get up to and over the $5,000 threshold. So while we don't know the facts in detail, that was probably enough.

The impairment of availability or integrity element would probably be satisfied, as well, although again we don't have much in the way of needed detail to know for sure. The leading case here is *Pulte Homes, Inc. v. Laborers' International Union of North America*, 648 F.3d 295 (6th Cir. 2011), which adopted a broad view of this requirement, holding that this is satisfied by "a transmission that weakens a sound computer system — or, similarly, one that diminishes a plaintiff's ability to use data or a system." The indictment alleges that Swartz's conduct impaired the working of the JSTOR database but doesn't give us much detail, so it's hard to be sure. Also, DOJ might be able to use JSTOR's decision to cut off access to JSTOR on MIT's network as an impairment of availability on the network. But I think this is a bit of a stretch, for two reasons. First, it's hard to know exactly where to place the responsibility for the impairment. Did Swartz cause it, or did JSTOR? And more significantly, does access to a particular service from some users really constitute an impairment of availability of the JSTOR computer itself? I'm not sure, but I'm wary of that argument. So the 1030(a)(5) charges are plausible, but we would need to know more facts to know for sure if they were justified.

*III. Conclusion*

My conclusion, at least based on what we know so far, is that the legal charges against Swartz were pretty much legit. Three of them are pretty strong; one is plausible but we would need to know more facts to be sure. Of course, there may have been reasons not to charge Swartz even though he had violated these statutes or to offer him a lenient plea.

I'll take on those questions in my next post. But to the extent we're focused on just what the law is, I think that what Swartz was alleged to have done fits pretty well with the charges that were brought.