Report to the President

MIT and the Prosecution of Aaron Swartz

Review Panel

Harold Abelson
Peter A. Diamond
Andrew Grosso
Douglas W. Pfeiffer (support)

July 26, 2013

Massachusetts Institute of Technology

L. Rafael Reif, *President*

77 Massachusetts Avenue, Building 3-208
Cambridge, MA 02139-4307 U.S.A.
Phone 1-617-253-0148

January 22, 2013

Dear Professor Abelson:

Since fall 2010, MIT has been involved in events arising from actions taken by Aaron Swartz to access JSTOR through the MIT computer network. I have asked you, and you have graciously agreed, to review MIT's involvement.

The purpose of this review is to describe MIT's actions and to learn from them. Your review should (1) describe MIT's actions and decisions during the period beginning when MIT first became aware of unusual JSTOR-related activity on its network by a then-unidentified person, until the death of Aaron Swartz on January 11, 2013, (2) review the context of these decisions and the options that MIT considered, and (3) identify the issues that warrant further analysis in order to learn from these events.

I trust that the MIT community, including those involved in these events, always acts with high professional integrity and a strong sense of responsibility to MIT. However, MIT tries continuously to improve and to meet its highest aspirations. It is in that spirit that I ask you to help MIT learn from these events.

Time is of the essence. Presently, many in the MIT community do not know what to make of the news reports on this matter. Out of respect for the value of analysis and reflection, MIT will wait for your report before commenting on the events that you will be examining. I urge you to conduct your review as rapidly as you can do so responsibly. I will be responsible for sharing your report with the MIT community and the public.

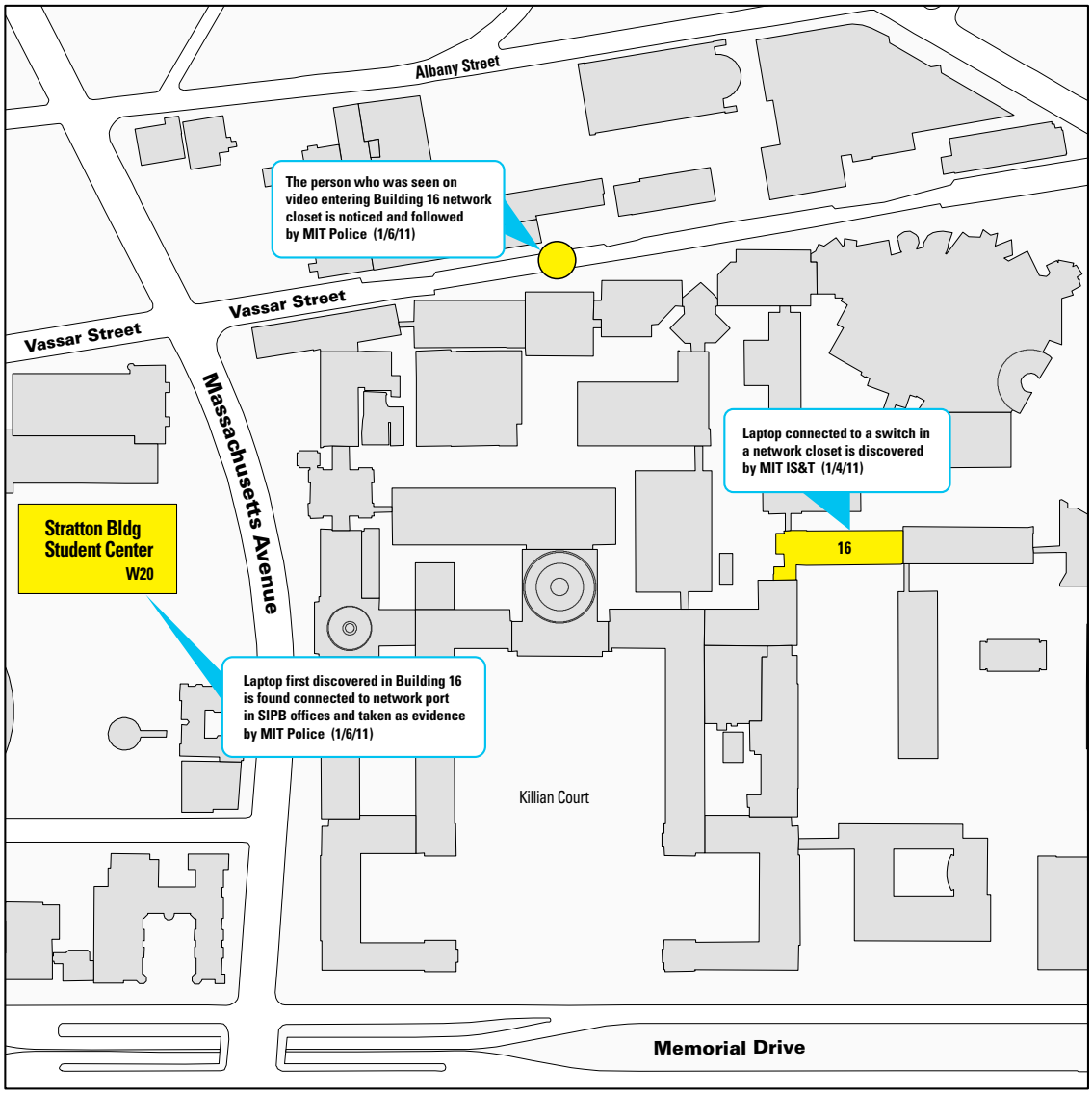
On behalf of MIT, I thank you in advance for the objectivity, analytic skill, and high sense of responsibility that you will bring to this task.

Sincerely,

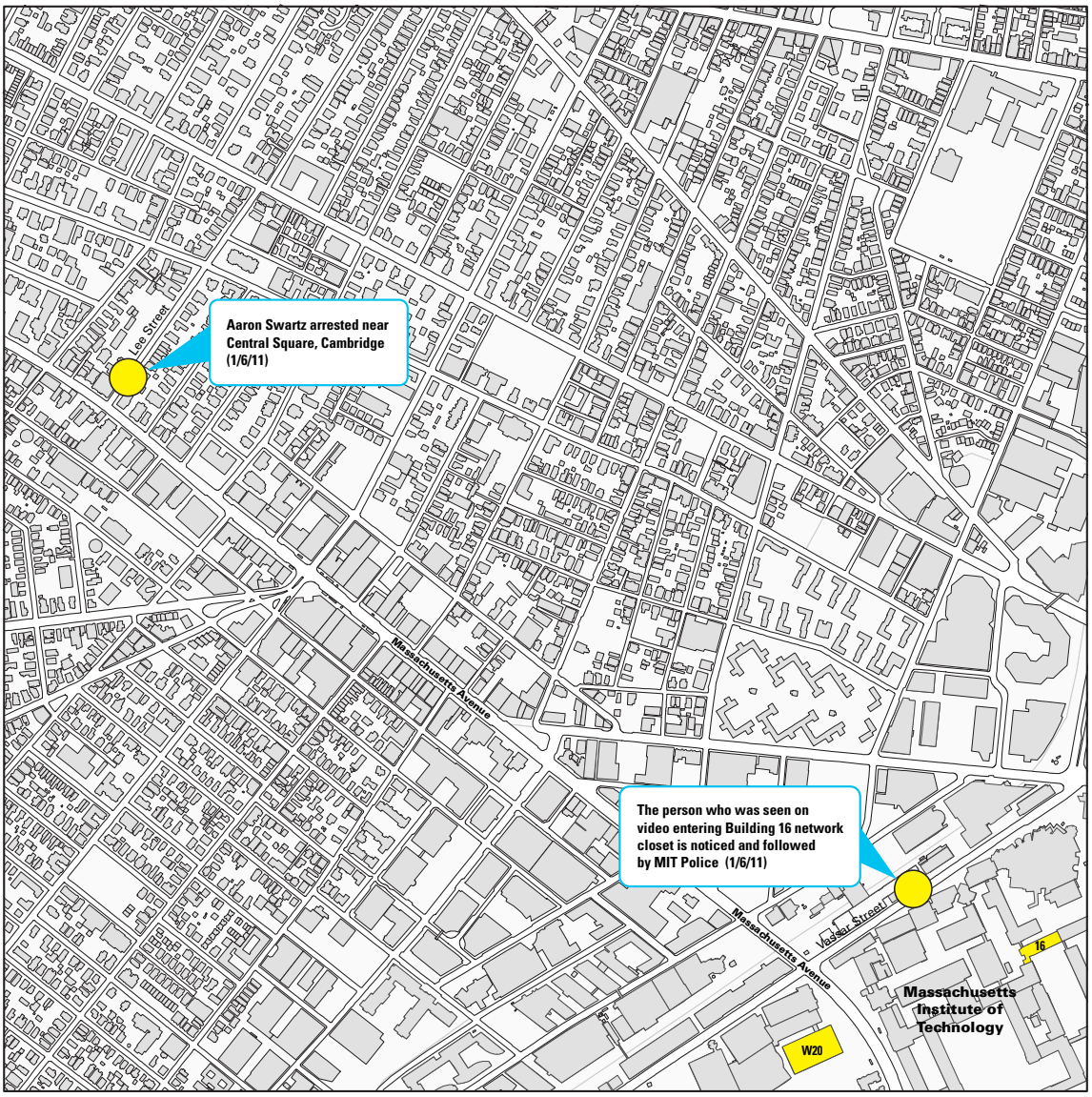
L. Rafael Reif
President

TABLE OF CONTENTS

ILLUSTRATIONS



Map 1. The MIT Central Campus



Map 2. The Central Square Area of Cambridge

INTRODUCTION

On January 6, 2011, Aaron Swartz was arrested by the MIT Police and an agent of the U.S. Secret Service, accused of breaking and entering for events that occurred on the MIT campus. In July 2011 he was charged in a federal indictment with multiple felony offenses, specifically violations of the Wire Fraud Act and the Computer Fraud and Abuse Act. On January 11, 2013, Aaron Swartz's partner found him dead in their New York apartment, a victim of suicide.

At the time of his death, Aaron Swartz was a 26-year-old computer programmer and an Internet celebrity—a former child prodigy who as a young teenager had worked alongside the leaders of the World Wide Web to create some of its basic technology for sharing information; an entrepreneur whose startup company became a key piece in a major news and entertainment service; an activist who co-founded an advocacy organization with more than a million members that organized petition drives for civil liberties and against censorship; and a Fellow at Harvard University's Safra Research Lab on Institutional Corruption.

Only Swartz knows why he committed suicide. However, for the final 24 months of his life, he was the subject of a vigorous investigation and prosecution by the U.S. Department of Justice, with an indictment and then a superseding indictment that could have resulted in years in prison. The charges stemmed from his actions, starting in fall 2010, when he surreptitiously downloaded massive quantities of scholarly journal articles from the JSTOR digital library through MIT's computer network.

Two days after the suicide, MIT President Rafael Reif asked Computer Science Professor Hal Abelson to lead the present review of MIT's involvement in the events, beginning with those in September 2010, when MIT first became aware of unusual download activity on its network, and continuing until Swartz's death in January 2013. The purpose of this review is to describe MIT's actions and consider what can be learned from them. In conducting the review, Abelson has been joined by MIT Economics Professor and Institute Professor Emeritus Peter Diamond; and Andrew Grosso, a Washington, D.C., attorney and former Assistant U.S. Attorney, with special expertise in computer law. When this report refers below to "we," "the reviewers," or the "Review Panel," it is referring to the three of us. MIT Assistant Provost for Administration Douglas Pfeiffer provided staff assistance. The process we used to gather information for this report is detailed in Appendix 4.[1]

---

[1] The Review Panel realizes that there has been significant controversy surrounding the events described in this report. We appreciate that many of the people involved have legitimate concerns about their privacy

Other than the announcement of the review on January 13, MIT has issued no statements before this report, in the interest of providing an account that is full, accurate, and fair. Since that time, we have received no further instruction from the MIT administration other than several public indicators that we should take as much time as we needed.

News of Aaron Swartz's death ignited a firestorm on the Internet. In the six months since our review began, there have been memorial services honoring Aaron Swartz in several cities, including one on Capitol Hill. The American Library Association posthumously awarded him its 2013 James Madison Award, and the Internet Society posthumously inducted him into the Internet Hall of Fame. A bill was introduced in Congress ("Aaron's Law") to revise the Computer Fraud and Abuse Act under which he was indicted. There has been a Congressional investigation and a petition to the White House demanding the firing of the prosecutors involved. There have also been several anonymous cyber-attacks—three of them against MIT—in protest of Swartz's prosecution, hate mail directed towards MIT employees and federal prosecutors involved in his case, and a hoax report of a shooter on campus that shut down MIT for a morning.

There have also been thousands of news articles and commentaries, many of them roundly critical of MIT. Reactions range from puzzlement, to headshaking disappointment, to anger, to dark hints of conspiracies. We hope this report, by laying out a full history of MIT's involvement, will put people in a better position to judge for themselves the plausibility of the various comments and positions taken, and to evaluate MIT's conduct.

Both the writing and the reading inevitably involve hindsight: how does one maintain a perspective uncolored by the shock and tragedy of Aaron Swartz's suicide, or—knowing of him and his accomplishments—by the realization that he was the person who did the downloading and who was then arrested? Just as we have tried to limit the effects of hindsight in the writing, we hope readers will do the same when interpreting our report.

---

and their security, and we know that some have even been personally threatened. Consequently, our report generally does not identify individuals by name. Many of these individuals have already been identified in court filings and other public documents, and we are fully aware that their names are readily discoverable on the Internet. Even so, we see no need to further erode their personal privacy. So as a rule, people in this report are identified by their role or position rather than by name. There are a few exceptions. In cases where including their names makes the narrative more understandable, we've named public officials—such as prosecutors, detectives, federal agents, judges, or police officers whose role in the events has already been described in public court filings. For some people actively involved in the events described, such as defense counsels for Aaron Swartz, we have used their names with their permission to do so. We have also named some people whose connections are only tangential to the events described in the report without having sought permission.

In brief, among our more significant findings are the following:

1. Until the arrest in January 2011, MIT was unaware that the person who engaged in the downloading of JSTOR's data beginning in September 2010 was Aaron Swartz. Until the arrest, MIT's concern was to stop the use of its network, by an unknown person, to download massive numbers of articles from the JSTOR database, which was in violation of MIT's licensing agreement with JSTOR and whose scale threatened the operation of the JSTOR network to the extent that JSTOR blocked MIT's access to JSTOR for three days. When, on the morning of January 4, 2011, MIT's network personnel located a laptop—covered by a cardboard box and plugged into a router in a basement data closet in a campus building—they were not sure with whom or with what kind of situation they were dealing, and they contacted the MIT Police. For the same reasons, the MIT Police sought forensic assistance from a detective in the Cambridge Police Department who had expertise in computer crime and with whom they had worked repeatedly in the past. The Cambridge detective, who was a member of the New England Electronic Crimes Task Force, responded to the call, accompanied by an agent of the U.S. Secret Service. While the inclusion of the Secret Service agent was not the intention of MIT, it was a recognized possibility. It was not until a few days later, when Aaron Swartz was arrested, that MIT learned the identity of the person involved in the JSTOR downloading. Thus, we find that MIT did not focus on Aaron Swartz at any time during its own investigation of the events that led to his arrest, and that MIT did not intentionally "call in the feds" to take over the investigation.

2. MIT never requested that a criminal prosecution be brought against Aaron Swartz. Early in the prosecution by the U.S. Attorney's Office in Boston (the "USAO"), MIT adopted a position of remaining neutral, with limited involvement. MIT hired outside counsel who had experience in criminal law and in the functioning of the Boston U.S. Attorney's Office; and MIT requested and received subpoenas for the production of documents. Some documents were turned over to the USAO prior to receiving a subpoena, but, for the reasons discussed in this report, this production did not violate federal laws.

3. In keeping with its stance of neutrality, MIT never issued a public statement about Swartz's prosecution or advocated publicly on his behalf, even though doing this was urged by Aaron Swartz's family and legal team and by two members of the faculty. One of the reasons for MIT's silence was the good-faith belief, based on private conversations with the lead prosecutor, that the Institute's opinion would have no effect on the prosecution, and that public

statements might make circumstances worse for Aaron Swartz. MIT did inform the prosecution that it was not seeking punishment for Swartz, and it did inform the defense that it was not seeking any civil remedy from him.

4. Before Aaron Swartz's suicide, the MIT community paid scant attention to the matter, other than during the period immediately following his arrest. Few students, faculty, or alumni expressed concerns to the administration. In preserving MIT's stance of neutrality and limited involvement, MIT decision-makers did not inquire into the details of the charges until a year after the indictment, and did not form an opinion about their merits. MIT took the position that *U.S. v. Swartz* was simply a lawsuit to which it was not a party, although it did inform the U.S. Attorney's Office that the prosecution should not be under the impression that MIT wanted jail time for Aaron Swartz. (MIT did not say it was actually opposed to jail time.) Among the factors *not* considered were that the defendant was an accomplished and well-known contributor to Internet technology; that the Computer Fraud and Abuse Act is a poorly drafted and questionable criminal law as applied to modern computing, one that affects the Internet community as a whole and is widely criticized; and that the United States government was pursuing an overtly aggressive prosecution. MIT's position may have been prudent, but it did not duly take into account the wider background of information policy against which the prosecution played out and in which MIT people have traditionally been passionate leaders.

Part I of this review recounts the actions MIT took from the first discovery of the downloading up to the time of Aaron Swartz's arrest. Part II reviews actions after the arrest by those involved other than MIT, in order to set the context for Part III, which describes MIT's own decisions and conduct between the arrest and the death of Aaron Swartz. Part IV highlights some of the options that MIT faced throughout this history. Part V provides some questions for the MIT community that the review panel believes should be starting points for discussion within MIT.

It was not part of our charge in this review to draw conclusions, but rather to determine facts and to consider what can be learned from this tragedy. Part V accordingly poses questions, not answers. These questions are for everyone at MIT, not just the Institute's leadership. They concern the kind of community that MIT is and the kind of community it could become. The questions reflect not only the particular events of the Aaron Swartz

case, but also the overall Institute circumstances and climate in which the events occurred. The most difficult questions challenge us to become better at negotiating the tension between prudence and passion, as great institutions must.

Cambridge, MA
July 26, 2013

Harold Abelson
Peter A. Diamond
Andrew Grosso
Douglas W. Pfeiffer

Part I: EVENTS LEADING TO THE ARREST

I.A Downloading of JSTOR Articles

The history of the events leading to the arrest of Aaron Swartz in January 2011 begins the previous fall with the JSTOR (Journal Storage) digital library, a service that licenses scholarly journals to numerous academic and research organizations, including MIT.[1]

On the evening of Saturday, September 25, 2010, JSTOR engineers noticed an extremely large number of requests for downloads originating from MIT. Overall, more than 450,000 articles spanning 560 journals were downloaded between 5:00 p.m. Saturday and 4:00 a.m. Sunday.[2] The volume of data transferred was enough to overload the affected JSTOR server. In response, JSTOR engineers temporarily blocked further downloads directed to the MIT Internet Protocol (IP) address issuing the requests.[3] But the downloading continued from a different IP address.

---

[1] See Appendix 6 for more information on JSTOR and the MIT Libraries.

[2] Ordinarily, when someone requests a download from JSTOR, the system pops up a window that refers to JSTOR's terms of use, and requires the user to click to confirm before the download can proceed. This not only notifies the user of JSTOR's terms, but also limits the rate at which automated downloads can be requested. In this case, however, the download script included a flag (acceptTC=true) that bypassed the acceptance step.

[3] In an effort to warn the person causing these downloads to stop, JSTOR's engineers caused a web page to be presented to the computer engaged in the downloading, reading:

Access Suspended—We noticed content downloading activity from your IP address (18.55.6.215) that appears to be in excess of what is allowed under our Terms & Conditions of Use. Please review our terms for more information about allowable uses. If you have additional questions or need other information, please contact JSTOR Support.

The next day, Sunday, September 26, 2010, JSTOR shut off access for the entire range of addresses (Class C network) containing the two addresses.[4] It sent an email to the MIT Libraries[5] ("the Libraries") notifying them of this fact, and explaining that JSTOR "rarely takes this level of response to abusive activity, but felt it necessary to maintain the stability of the Web site for other institutions and users." JSTOR further noted in that email that the manner in which the download requests came into its system "clearly indicates robotic harvesting of PDFs [articles] which violates our Terms & Conditions of Use." Reflecting its contractual agreement with JSTOR, the Libraries began to work with JSTOR in an effort to determine the source of the downloading and stop it from continuing.

JSTOR sought MIT's assistance to prevent the incident's recurrence. The Libraries responded: "We're investigating this case and, because the origin of the activity was a guest visiting MIT, we believe that it will not recur. We hope that you will be able to restore the Class C range that has been suspended on this information." In response, JSTOR turned all of MIT's IP addresses back on, and decided to watch.

To provide some context for this event, we note that the Libraries handled 65 excessive use incidents during the 2010–2011 academic year. Typically, when an excessive use case is reported that is determined to originate from within MIT's network, the Libraries report this to either the MIT Information Services and Technology (IS&T) network security team[6] or MIT's "Stopit" group, which deals with inappropriate behavior that occurs electronically. The Stopit group's general response is to send the offender a warning email message. This is almost always all that is needed to get people's attention and have them stop whatever it was they were doing that caused the problem. In this case, however, the computer was registered to a visitor, and the registrant used an anonymous

---

[4] The first IP address was 18.55.6.215, and the second address was 18.55.6.216. The blocked range consisted of all IP addresses beginning with 18.55.6 followed by a number from 0 through 255. Such a range (four numbers, with the first three fixed, and the last one taking on any value from 0 to 255) is called a Class C network.

IP (Internet Protocol) addresses specify the network port where the device is attached. They are typically automatically assigned, when the device is attached, by a network service called a DHCP (Dynamic Host Configuration Protocol) server, although people with sufficient computer skills can change the IP address (as was done here). In addition to the IP address, each device has a MAC (Media Access Control) address, which uniquely identifies the device's hardware network interface itself (essentially, the device itself, as opposed to where it is attached to the network). MAC addresses are typically assigned by the device manufacturer, although these, too, can be changed under program control. The network DHCP server maintains a log, called a DHCP log, which records the IP address assigned to a MAC address, as part of the DHCP process. At MIT, an IP address will often identify the building where network device is located.

[5] Email sent Sunday, September 26, 2010, at 12:31 p.m.

[6] Most cases of excessive downloading are due to misappropriation of MIT credentials, in which case the true MIT user is asked to change his/her password.

email address that could not be contacted.[7] (As described in section I.E.1, guests may register to use the MIT network by supplying a name and an email address as contact information, and they obtain a registration that is valid for a limited time period.) IS&T therefore disabled the registration of the MAC address used by the offending computer, expecting that this would be a sufficient deterrent to further activity.

Two weeks later, on Saturday, October 9, 2010, during the Columbus Day weekend, a second, similar incident occurred: a visitor downloaded more JSTOR articles, using a slightly modified MAC address.[8]

This time, the requests and downloads stimulated a cascade of failures that brought down multiple JSTOR servers. Half the servers in one data center failed, and JSTOR engineers feared that the entire service might go down worldwide. Moreover, the requests seemed to be coming from thousands of machines.[9]

JSTOR's response was to shut down service, at approximately 11:15 p.m. on October 9, 2010, to all MIT's IP addresses, that is, the entire Class A network,[10] doing so quickly enough that only about 8,000 articles were downloaded during this incident. JSTOR observed that the downloaded articles were not limited to a specific discipline, but were sequential across JSTOR's entire database. To JSTOR, this indicated "a concerted effort is being made to download the entirety of the JSTOR archive." JSTOR notified MIT Libraries of its findings by email, and spoke directly with personnel at the Libraries about its concerns.

---

[7] The addresses supplied with the registrations were generated by Mailinator (<http://www.mailinator.com>), a service that creates on-the-fly temporary email addresses.

[8] (See footnote 4 for an explanation of MAC addresses.) The initial MAC address was 00:23:5a:73:5f:fb, registered on September 24, 2010, to a "person" named "Gary Host." The second (slightly modified) MAC address was 00:23:5a:73:5f:fc, registered on October 2, to "Gary Host." These were the same machine, as evidenced by the similarity of MAC addresses and the fact that they presented the same DCHP client ID, "ghost-laptop," to the DHCP server. The MAC address provided is consistent with this being an Acer laptop. (See Appendix 7 for information on DHCP.) In addition, there was a second machine registered, on October 8, 2010, to "Grace Host" with the MAC address 00:17:f2:2c:b0:74. This machine had the client ID "ghost-macbook," and the MAC address is consistent with this being an Apple MacBook. There was also a third registration, on October 22, 2010, with user name "Grace Host" and client ID "ghost-laptop," with MAC address 00:4c:e5:a0:c7:55, and again a registration on November 28, 2010, with MAC address 00:4c:e5:a0:c7:56. These registrations are for the Acer laptop that was discovered in the closet. (See section I.B below.) The MAC addresses used here are invalid: they do not correspond to any manufacturer ID. This is apparently the same "ghost-laptop" machine as was registered on September 24. One can conjecture that the owner, having seen the first MAC address blocked, and the second, slightly modified address also blocked, set the machine to a radically different MAC address.

[9] In actuality, there was only one machine. It deleted its JSTOR cookie after each download, disconnected, and then re-accessed JSTOR, resulting in a new cookie being placed on the machine each time this occurred and making it appear that this was a new machine for each access.

[10] That is, the range of IP addresses starting with 18 and followed by three numbers (i.e., 18.x.x.x).

Both MIT and JSTOR were anxious for service to MIT to be restored. JSTOR believed that it could monitor the system and stop further incidents because it had been able to notice and stop the latest one after only 8,000 articles had been downloaded. Based on this, JSTOR agreed to restore service to MIT and did so on Tuesday, October 12, 2010, after three days of the entire campus being blocked. At the same time, IS&T blocked access from the individual MAC address most recently associated with the downloading. Meanwhile, IS&T staff were able to determine that the downloading activity had originated from the Dorrance Building (Building 16), an academic building in the central campus.[11]

Also on October 12, the Director of the MIT Libraries reported to MIT's Academic Council[12] that a cyber-attack of the JSTOR database had caused a weekend shutdown of JSTOR to the entire campus.

Following the suspension of service to the entire MIT campus during October 9 through 12, JSTOR decided to monitor closely for additional downloading activity and be prepared to suspend access as necessary.

On the evening of December 26, 2010, JSTOR again noticed excessive downloading from MIT, originating from a new IP address. Significantly, this most recent downloading had been going on for some time, beginning in late November, but JSTOR did not realize this fact until much later. The manner of accessing downloads had been slowed and altered in such a way that JSTOR's monitoring systems did not identify that the robotic harvesting had resumed.[13] This time, JSTOR noted that the downloading activity originated from the same Class C network that IS&T had identified earlier as being in Building 16.[14] JSTOR promptly notified the MIT Libraries about the new incident, by email, on the same evening, identifying Building 16 as the apparent location of the IP address. In this email, JSTOR also made the following request to MIT: "We are

---

[11] The September 25, 2010, downloading was also from a wired connection in Building 16. IS&T did not pinpoint the exact location in either September or October 2010.

[12] MIT's Academic Council consists of the Institute's senior leadership plus the elected Chair of the Faculty. It is chaired by the President and meets weekly during the academic year to confer on matters of Institute policy.

[13] There were over 4.3 million downloads during the period from late November through Swartz's eventual arrest on January 6.

[14] Beginning December 26, 2010, JSTOR took several actions to stop or at least impede the downloading. First, it blocked an entire Class C range of addresses for Building 16. JSTOR also kept open the one IP address that it observed the machine using, 18.55.6.240, and moved access for this address to a server separate from the rest of its network. Through this server, JSTOR responded to the machine's requests by downloading strings of zeros and meaningless articles, in the expectation that: (1) the machine would not notice and would continue to download worthless material; and (2) this would slow any remaining downloading that might take place. However, the machine had also been registered with an IP address of 18.55.7.240, that is, with a 7.xxx instead of 6.xxx and entirely outside of the Class C range of IP address that JSTOR had blocked. The downloading continued unimpeded, without JSTOR realizing it.

requesting that every effort be made to identify the individuals responsible and to ensure that the content taken in this incident and those previously mentioned is secured and deleted." An email sent the following day from JSTOR to the Libraries re-emphasized the urgency of the situation: "Once again, we are seeing extreme unauthorized activity from MIT. We really need to find out who is doing this; it is malicious and intentional and as best we can tell is coming from inside of MIT."

Employees of the MIT Libraries had been furloughed for the winter holidays, and thus they did not see the messages JSTOR sent on December 26 and 27, 2010, until Monday, January 3, 2011.[15] On the morning of January 4, the Libraries informed JSTOR that MIT did not expect to be able to identify the individual involved in these incidents based on the information available at that point.[16]

I.B Discovery of the Laptop

At approximately 3:00 a.m. on January 4, 2011, IS&T staff sent an email to its network engineers requesting that they trace the exact location in Building 16 of the computer using the IP address. An IS&T network engineer began to search when he arrived for work in the morning, going to Building 16 and checking the basement closet containing the building's network switches.[17] Around 8:00 a.m., he entered the closet and saw a cable connected to a network switch and leading to a cardboard box on the floor. He lifted the box and saw a laptop computer. He telephoned an IS&T network manager, who quickly joined him at the closet.

---

[15] The MIT Libraries were closed for business from 6:00 p.m. Wednesday, December 22, 2010, through Sunday, January 2, 2011. The majority of these days were regular or special Institute holidays. However, December 27, 28, and 29, 2010 were furlough days, during which time the staff were required by the Libraries' administration to take involuntary, unpaid leave as a cost-saving measure to meet budget reductions. Furloughed staff were explicitly prohibited from working during furlough days. Two technical staff members were asked to defer their furlough days to another time, so that basic technical support to the Libraries' networked resources could be provided. Their directives included that (a) access to licensed resources was to be kept available, both on and off campus, to the degree possible; and (b) any outages caused by problems at MIT's end were to be resolved promptly. In the unlikely event that a major aggregator or database should cut off service to MIT during this time, one of the two staff members was responsible for making best efforts to work with the vendor to resolve the outage. This staff member was copied on JSTOR's email of December 26, 2010, to the Libraries but did not respond. The Libraries wrote to JSTOR on January 3, explaining that people had been on furlough and had not seen the JSTOR's prior messages. This January 3 message was the Libraries' first response to JSTOR's December 26 and 27 emails.

[16] The January 4 email also suggested to JSTOR that it block the entire 18.55.xxx.xxx Class B network, since the downloading was coming from two different Class C networks. (See footnote 14.) At the time the email was sent, the Libraries did not know that that laptop had been discovered a few hours before.

[17] The closet had two doors connected in the middle by a common lock, with both doors swinging outward when opened. He used his key to enter the basement closet; however, he does not remember whether the doors were actually locked. According to this network engineer, even when locked, the closet could be opened by pulling on both doors simultaneously because the locking mechanism had been damaged.

Over the next hour, the two engineers contacted IS&T management and the IS&T Security Team. The Security Team also consulted MIT's Office of the General Counsel (OGC). At 9:45 a.m. IS&T management notified the MIT Police that a laptop connected to a network switch had been found in an electrical closet in Building 16. Two additional IS&T staff members arrived. Minutes later, uniformed MIT Police officers arrived in Building 16 and were posted in the basement hallway. A network engineer then used an MIT laptop to connect to the network switch, in order to monitor the traffic (packet stream) to and from the suspect laptop.[18] Through this monitoring, the Security Team observed the downloading of data.

Another member of the MIT Police arrived, accompanied by a photographer. They took photographs of the closet, including the box, the laptop, and a hard drive sitting under the laptop. The MIT Police decided that the situation required expertise in computer crime and forensics, which they did not have. They therefore telephoned the Cambridge Police Department detective who is their normal contact for assistance with computer-related crime activity.[19]

The Cambridge detective they contacted was a member of the New England Electronic Crimes Task Force.[20] When he received the call for assistance from the MIT Police, the detective was working at the Task Force field office in a federal building in Boston, together with other law enforcement officers whose agencies participate in the Task Force. He responded to the call, accompanied by two other Task Force members: a special agent[21] of the U.S. Secret Service; and a detective from the Boston Police Department. They arrived at the Building 16 closet around 11:00 a.m.

We note that no one from MIT called the Secret Service. The MIT Police contacted the Cambridge detective by calling him on his individual cell phone. The special agent became involved because he accompanied the Cambridge detective. As a Task Force member, the detective would sometimes respond to calls alone, and sometimes respond in

---

[18] This monitoring of the switch was accomplished by one of the engineers plugging a cable (connected to his MIT laptop) into a port on the switch. At no time did he or anyone else from MIT in any way connect to the suspect laptop itself or to its cable. With very small exceptions, the only communications observed were those to and from the suspect laptop. (See Appendix 7.) The packet stream was preserved on the MIT laptop and later made available to the Secret Service special agent who became involved in the investigation.

[19] The MIT Police typically make calls to the Cambridge Police for assistance in computer-related matters about six times a year. In none of these incidents were federal agents part of the response.

[20] The New England Electronic Crimes Task Force (<http://www.secretservice.gov/ectf_newengland.shtml>) is a Boston-based alliance organized by the Secret Service with participants from federal, state, and local law enforcement, as well as private industry and academia, to investigate electronic crimes, including computer system intrusion.

[21] All federal agents who are authorized to carry firearms in the course of their normal duties are referred to as "special agents." Agents of the Secret Service, as well as most federal law enforcement agents, have the title of "special agent."

the company of other members of the Task Force. The MIT Police were aware that other members of the Task Force might accompany the detective, and that Task Force members included Secret Service agents.

When they arrived, the suspect laptop was still downloading data. Also, during the monitoring, the MIT network engineers had observed that the laptop was being queried from several sources, including on one occasion an IP address located in China. This information was communicated to the law enforcement officials. The fact that someone or some entity in China could be involved initially raised concerns that this might have been part of an international matter.[22]

The special agent attached a USB device to the suspect laptop in an attempt to copy the hard drive, but this attempt was unsuccessful. Crime scene investigators from the Cambridge Police Department arrived and took fingerprints from the laptop and hard drive.[23] The agencies and personnel worked together in a cooperative fashion, with no law enforcement group taking orders from any other.

The law enforcement group decided to leave the laptop and hard drive in place to see if the person who had set it up would return. Because it was not feasible to continuously post MIT Police officers in the basement corridor for an indefinite period of time, and doing so would reveal the surveillance of the closet, the decision was made to install a video camera in the closet that could be monitored from elsewhere within MIT. IS&T installed the camera at the request of the MIT Police. At around 3:00 p.m., the basement closet was restored to the way it was found, with the exception of the camera having been installed. IS&T engineers relocated the MIT laptop they were using to another room and reconnected it to the MIT network to continue monitoring the network traffic to and from the suspect laptop, and everyone left the closet area.

Half an hour later, an individual was seen on the video camera entering the basement closet. He changed the hard drive attached to the laptop, and put the old one into a backpack. Some of the law enforcement officers went to the closet to try to apprehend him, but he had left before they could arrive. No one recognized the person in the video. Still photos showing the suspect were taken from the video and provided to the MIT Police.

During the morning's activities in the basement closet, the special agent had asked for whatever electronic records MIT might have on the matter. As it is IS&T's protocol to obtain approval from MIT's Office of the General Counsel (OGC) before releasing

---

[22] Ultimately, MIT concluded that the communication from the IP address located in China was a—not unusual—"pinging" attempt by someone or some entity in China to determine what computer systems at MIT were available and accessible, and unrelated to the activity of this laptop.

[23] MIT Police regularly rely on Cambridge Police for latent fingerprint collection.

information or materials to outside law enforcement agencies, IS&T contacted the OGC, which responded that it was appropriate to comply with the agent's request in view of the fact that law enforcement was conducting an investigation into what was potentially ongoing criminal activity of unknown scope, and it did not appear to OGC that such information would disclose personally identifiable information.[24]

IS&T turned over the following information to the Secret Service, at its request, on the afternoon of January 4, 2011:

1. Network flow data, which is made up of logs showing which IP addresses communicated with which IP addresses; when the communication took place; and how much data was transferred.

2. DHCP (Dynamic Host Configuration Protocol) logs, which are records of requests from computer clients for the DHCP service to assign IP addresses. These records contain MAC addresses, IP addresses, and when clients acknowledge the receipt of addresses.

3. RADIUS (Remote Authentication Dial In User Service) logs, which record requests to use various network services.

In addition, the following was made available to the Secret Service, at its request, and was provided to the special agent on January 25, 2011:

4. The packet stream captured by the MIT network engineer using his laptop, as described above; this consisted of copies of the JSTOR downloads and associated control information—some 87 gigabytes in all.

These categories of items, Nos. 1 through 4, were provided by MIT to the Secret Service without a subpoena having been issued to MIT. Thereafter MIT provided additional documents to the Office of the U.S. Attorney in response to grand jury subpoenas.[25] A more detailed description of these items is available in Appendix 7. (Appendix 10 addresses legal issues concerning production of the records.)

---

[24] At this time, IS&T knew about the JSTOR downloading, but they also were concerned that the laptop might be performing other actions.

[25] One such item—consisting of six records from the network registration database showing registration for Gary Host and Grace Host in September and October 2010—was provided by MIT in September 2011, under the impression that it was doing so in response to a grand jury subpoena. However, at the time those records were produced, this subpoena (issued on January 27, 2011) was apparently no longer valid.

I.C Events of January 6, 2011: The Arrest

At about 12:30 p.m. on Tuesday, January 6, someone entered the closet, as was recorded by the video camera. As he entered, he covered his face with a bicycle helmet, removing it after he entered and the doors had closed. The individual removed the laptop and hard drive and then left the closet. [26] When the laptop was disconnected, the port status of the switch changed, and a monitoring script sent an email to the phone of one of the IS&T engineers, who was not on campus at the time. The IS&T engineer notified the MIT Police and other network engineers, but no one was able to reach Building 16 in time to stop or intercept the person who had entered the closet. Later the same afternoon, the suspect computer's MAC address reappeared in MIT's network logs, showing that it was connected, first in MIT Building 4, then subsequently in the Stratton Student Center (Building W20[27]), in the offices of MIT's Student Information Processing Board (SIPB—MIT's student computing group).[28]

At approximately 2:00 p.m. an MIT Police officer was driving to the Stata garage after his shift in an unmarked police cruiser. He was familiar with the investigation and had been informed by radio that the laptop had been removed from the basement closet. He had seen the January 4 video of the suspect, as well as stills made from the video, and he had a still with him in his cruiser. On Vassar Street, near Massachusetts Avenue, he saw a cyclist pass him heading in the opposite direction. Based upon the stills and video, and given the backpack and clothes the cyclist was wearing, the officer observed that the cyclist matched the description of the suspect from the basement closet. He made a U-turn to follow the cyclist, who turned onto Massachusetts Avenue and proceeded north towards Harvard Square. When the officer reached the cyclist and pulled alongside, he rechecked the still photos that he had in his car and concluded that the cyclist was in fact the person in the photos. He immediately called his department for backup. A second

---

[26] A few minutes before this person entered the closet, two MIT employees were seen on camera, standing in the opening of the closet doorway and then leaving. It is possible that the person utilizing the laptop saw these persons leaving the closet and, for that reason, decided to obscure his face while he was in the hallway, still walking to the closet, to avoid being identified by them. It is also possible that his observation of these employees is why he decided to move the laptop out of the closet and to another location. We note that this is speculation on the part of the Review Panel.

[27] See the maps in the front matter.

[28] When the laptop was disconnected from the network and removed from the closet, the IP address that it had been using was released by the network. The DHCP server network reassigned this address to another user, in another part of the building. Since the IP address was being monitored by IS&T, this initially led to some confusion as to where the suspect initially went, and where he initially reconnected his laptop.

MIT Police officer, accompanied by the special agent, responded by car from the MIT Police station.[29]

When the cyclist reached the north side of Central Square, the officer who was following him decided to pull ahead of him and stop him to ascertain his identity.[30] While exiting his car, the officer held his credentials so that they could be seen and motioned for the bicyclist to stop. The bicyclist complied. The officer explained that he was an MIT Police officer and wanted to speak with him. The cyclist first said that he didn't speak with strangers. The officer again displayed his badge, as well as his photo ID. The cyclist then said that MIT Police were not "real cops" and refused to talk to the officer. At that point the cyclist dropped the bicycle to the ground and started running back toward Central Square, on Massachusetts Avenue. The officer chased him briefly, but the individual was outrunning him, and the officer returned to his car, made a U-turn, and followed, maintaining visual contact. The suspect slowed to a walk, and the officer, still in his car, watched and followed him.

The first MIT Police officer radioed the second and told him where the suspect was located. Once near the suspect, both MIT Police officers and the special agent left their vehicles and chased the suspect around parked cars. They apprehended and handcuffed him.[31]

At this time, the officers still did not know the suspect's identity. One of the officers called the Cambridge Police, who arrived and took the suspect to the Cambridge Police Department for booking. There, he was identified as Aaron Swartz. Aaron Swartz refused to talk to the police. He made a phone call to his friend Quinn Norton, who arranged for another friend to rush to the police station with bail money. Shortly thereafter an attorney from the firm of Good & Cormier arrived at the Cambridge Police Department, completed the paperwork for Aaron Swartz's bail, and departed with him.

I.D Events of January 6, 2011: Seizure of the Laptop

Later on January 6, 2011, after Aaron Swartz was apprehended, members of IS&T, accompanied by MIT Police and the special agent, went to the SIPB offices in the Stratton Student Center to look for the laptop. Together, they found the laptop with an external hard drive, plugged into a network jack. The special agent examined the laptop and the participants decided that there was no feasible way to collect evidence from the

---

[29] When the backup call was received, the special agent was reviewing the relevant video at the MIT Police station. He joined the MIT backup officer.

[30] The MIT Police are deputized under the Middlesex County Police Department.

[31] Aaron Swartz was arrested in connection with an alleged violation of state law, not federal law. The special agent participated in the arrest.

laptop while it was operating. It was disconnected and turned off. An MIT detective took the laptop and the external hard drive as evidence. On February 3, 2011, custody of the laptop and hard drive was transferred from the MIT Police to the Cambridge Police.

I.E Access to the MIT Network

As it is relevant for the post-arrest narrative, we briefly describe MIT's procedures for network access and review how Aaron Swartz obtained access to the MIT network and to JSTOR.

I.E.1 Connecting to the MIT network

MIT community members who want to use the wired network register by presenting an MIT user name and password that were issued to them when they began employment, or first registered as students, or were given a formal appointment at MIT, and they obtain permanent registrations for their computers. All other individuals—"guests"—who want to connect to MIT's wired network supply a personal name and an email address as contact information, and they obtain a registration that is valid for up to 14 days a year of cumulative use, as explained on IS&T's information page:[32]

> IS&T offers short-term network service to campus guests. Guests are allowed up to fourteen days of network service when they register on the wired MIT network (MITnet) . . . .
>
> For wired connections, plug the Ethernet cable into the computer and to an MITnet network drop . . . .
>
> The machine needs to be configured for DHCP (obtaining an IP address automatically) . . . .
>
> Once the equipment is ready to connect, open a web browser and point it to any web page. A page will appear, prompting to select your registration option. After selecting Visitor registration, the returned page will display the MITnet Rules of Use, followed by a screen requesting the visitor's contact information, number of days of connectivity, and the event for which they are on campus.
>
> Visitors can register between one and five (consecutive) days at a time, up to fourteen days per year.

[32] See Network Connectivity for MIT Guests, <http://ist.mit.edu/network/netguests>.

More precisely, the requirement to register is triggered when the computer asks MIT's DHCP server to issue it an IP address. It is also possible to configure a computer to use a self-assigned "static IP address," in which case there will be no registration request (provided that the static IP address is in an appropriate range, and does not conflict with an address that has already been assigned). MIT's procedure is that static IP addresses should be requested through IS&T, so as to avoid conflicting address assignments, which would result in disruption of service.[33]

As noted above (footnote 8), Aaron Swartz registered five times in 2010: September 24, October 2, 8, and 22, and November 28. When the laptop was located in January 2011, it had a static IP address. At some point,[34] Swartz had switched from using DHCP-provided IP addresses to using a static self-assigned IP address.[35]

I.E.2 JSTOR and eControl

MIT operates a very open network. Anyone can come onto campus and plug their computer into an MIT network port, or connect to the wireless network.[36] Connecting to the wired network, and getting connected automatically, requires registering the computer the first time it is plugged in. Connecting to MIT's wireless network does not require registration.

Prior to January 2011, any computer connected to the MIT network could access JSTOR. In the wake of the October 2010 downloading incident, and as a direct result of that incident, the Libraries and IS&T decided to deploy an authorization system for JSTOR called "eControl" that had been designed by the MIT Libraries to more narrowly restrict access by the MIT community to certain electronic databases. Under eControl, requests to access JSTOR would require a valid MIT certificate and be verified against MIT's Human Resources directory, and only MIT faculty, students, or staff—not guests—would be granted access to JSTOR. Guests seeking access to JSTOR would now have to come to the MIT Libraries and use a library computer there.

MIT was prepared to implement eControl as early as October 2010. JSTOR and MIT were mindful that an abrupt change would diminish user convenience for the MIT community. JSTOR asked MIT to delay deployment of eControl to allow JSTOR to add an explanatory message to the JSTOR web page that would advise MIT users of the change, and redirect them through the eControl process. JSTOR informed MIT that this

---

[33] See "Request an IP Address/Host Name," <http://ist.mit.edu/network/ip-request>.

[34] MIT is not sure when, as there is no MIT system of record that would have indicated this.

[35] He used two different addresses, 18.55.6.240 and 18.55.7.240.

[36] MIT's framework for network security follows the general principle that, while access to individual resources on the network could be restricted, access to the underlying network should be as open as possible. This reflects a general computer system design methodology called the End-to-End Principle.

change would not be ready to implement until after December 18, effectively putting off the planned activation of eControl until after MIT's winter holiday break.

On the morning of January 3, MIT and JSTOR agreed to expedite the implementation of eControl, and the system was activated on January 10, 2011. Since then, guests at MIT can access JSTOR only from certain workstations located in the libraries.

Part II: BACKGROUND ON AARON SWARTZ AND LEGAL EVENTS FOLLOWING THE ARREST

Part I of this review covered events from the start of the JSTOR downloading in September 2010 through the arrest of Aaron Swartz in January 2011. Part III will take up a discussion of MIT's actions after the arrest. Here, in Part II, we describe the background against which MIT's actions played out. Apart from providing information, MIT had little role in the events described in this part of the report. But these events add important context for understanding MIT's decisions and actions described in Part III.

We first provide some perspective on Aaron Swartz and his interactions with the MIT and Harvard communities. We then review the legal proceedings in which he was involved as a result of his arrest, which included multiple prosecutions, multiple indictments, and several different attorneys. Finally, we describe the settlement agreement between Aaron Swartz and JSTOR negotiated and executed during the period leading up to the indictment handed up in July 2011.

II.A Background on Aaron Swartz

Aaron Swartz was a computer programmer and activist, well known in the Internet, civil liberties, and technological–academic communities. He was 24 at the time of his arrest. By the age of 14, he had played an instrumental role in the development of the web publishing format RSS, the metadata schemes for Creative Commons, and several other

cutting-edge Internet technologies. By the age of 19 he had started and sold a successful web-publishing company.[1] He was also the cofounder of Demand Progress, an Internet blog and activist group self-described as focusing on civil liberties, civil rights, and government reform.[2]

II.A.1 Aaron Swartz in Cambridge

Aaron Swartz was neither a member of the MIT staff, nor an enrolled student nor alumnus, nor a member of the faculty. He was a regular visitor to the MIT campus and interacted with MIT people and groups both on campus and off. His web-publishing startup was developed with the help of an entrepreneurship accelerator company "boot camp" that arranged for him to be housed on the MIT campus for the summer of 2005.[3] After a short period in San Francisco, he returned to Cambridge in 2006 and lived in an apartment on Massachusetts Avenue in Central Square, between Harvard and MIT. He was a member of MIT's Free Culture Group,[4] a regular visitor at MIT's Student Information Processing Board (SIPB), and an active participant in the annual MIT International Puzzle Mystery Hunt Competition.[5] Aaron Swartz's father, Robert Swartz, was (and is) a consultant at the MIT Media Lab. Aaron frequently visited his father there, and his two younger brothers had been Media Lab interns.

Aaron Swartz was a respected contributor to the World Wide Web Consortium's Semantic Web, HTML, and TAG (Technical Architecture Group) activities. He attended gatherings of the Semantic Web working group that met at the MIT Computer Science and Artificial Intelligence Laboratory, and he was an invited speaker at one of the gatherings in 2008.

In 2010, Aaron Swartz became a research fellow at Harvard University's Edmond J. Safra Center for Ethics,[6] invited to conduct experimental and ethnographic studies of the political system and to prepare a monograph on the mechanisms of political corruption.

---

[1] The company was Infogami, which was used to support the Internet Archive's Open Library Project. Infogami later merged with Reddit, which was subsequently acquired by Condé Nast.

[2] Since the suicide, there has been an enormous amount of information published about Aaron Swartz, and speculation about why he downloaded the JSTOR material and about factors contributing to the suicide. See for example, Larissa McFarquhar, "Requiem for a Dream," in the *New Yorker,* March 11, 2013, <http://www.newyorker.com/reporting/2013/03/11/130311fa_fact_macfarquhar>; Wesley Yang, "The Life and Afterlife of Aaron Swartz," *New York Magazine*, February 8, 2013, <http://nymag.com/news/features/aaron-swartz-2013-2/>; Quinn Norton, "Life Inside the Aaron Swartz Investigation," *The Atlantic*, March 3, 2013, <http://www.theatlantic.com/technology/archive/2013/03/life-inside-the-aaron-swartz-investigation/273654/>; and many others.

[3] The accelerator company was Y-Combinator (<http://ycombinator.com>). Aaron Swartz was housed in Simmons Hall. See Swartz's web log of June 11, 2005, for his comments about arriving in Cambridge.

[4] <http://freeculture.mit.edu/>, now inactive.

[5] MIT Mystery Hunt, <http://www.mit.edu/~puzzle/>

[6] <http://www.ethics.harvard.edu>

He had an office at the Center, and he was a regular contributor to discussions and activities there.

After Aaron Swartz's arrest, Harvard suspended his fellowship and banned him from the Harvard campus, pending the outcome of an investigation into whether he had also used Harvard's computers or network for similar activities.[7] MIT took no action itself, but at Aaron Swartz's arraignment on January 7, 2011, Cambridge District Court Judge Thomas ordered him to stay away from MIT property as part of the conditions of release.[8] U.S. Magistrate Judge Dein imposed the same ban as a condition of Aaron Swartz's release at his initial appearance and arraignment for the federal indictment on July 19, 2011.[9] At the time of the federal arraignment, Aaron Swartz was residing at two locations: one in Brooklyn, New York, near his employment as an independent contractor in New York City; and the other in Cambridge, Massachusetts.[10]

II.A.2 Possible motives for downloading

As far as the Review Panel knows, Aaron Swartz made no statement after his arrest regarding what he had planned to do with the downloaded documents. The Review Panel views the question of what he intended to do with the information that he was downloading from JSTOR as remaining open.[11] Speculations about his motives reference a statement about free information to which he contributed, as well as two previous, large download experiences.

The federal indictment states that the downloading was "with the purpose of distributing a significant proportion of JSTOR's archive through one or more file-sharing sites." That is, the alleged motive is that Aaron Swartz intended to place the material on the Internet so that it could be freely distributed around the entire globe. In support of this

---

[7] Although the investigation apparently did not find that he did this, his fellowship expired before this finding was made, and before the ban was lifted. Harvard's OGC declined to comment for this review.

[8] Recall from Part I that Aaron Swartz was arrested under Massachusetts Law.

[9] The Federal District Court conditions of release are at <http://ia600504.us.archive.org/29/items/gov.uscourts.mad.137971/gov.uscourts.mad.137971.6.0.pdf>. As far as the Review Panel has been able to determine, the Cambridge District Court and Federal Court bans were imposed at the recommendations of the District Attorney and the federal prosecutor, respectively, and no one in the MIT administration asked for them or knew about them. The federal conditions of release also included the requirement that Aaron Swartz "undergo medical or psychiatric treatment as directed."

[10] Defendant's Motion for Leave to Change Residential Address, Doc. 15 (filed September 8, 2011), *United States v. Swartz*, Case No. 1:11-cr-10260-NMG.

[11] Also open is the question as to why Aaron Swartz used the MIT network for the downloading, as opposed to the Harvard network, to which he already had registered access. Lawrence Lessig, Director of the Safra Center and Professor of Law, Harvard Law School, suggests that Aaron Swartz did the downloading at MIT so as not to create trouble for Lessig and the Safra Center. (Lawrence Lessig on "Aaron's Laws—Law and Justice in a Digital Age," <http://www.youtube.com/watch?v=9HAw1i4gOU4&feature=player_embedded>.)

interpretation of his purpose, the government pointed[12] to a "Guerilla Manifesto" he posted on the Internet in 2008. This "manifesto" included the following:

> We need to take information, wherever it is stored, make our copies and share them with the world. We need to take stuff that's out of copyright and add it to the archive. We need to buy secret databases and put them on the Web. We need to download scientific journals and upload them to file sharing networks. We need to fight for Guerilla Open Access.[13]

Federal law enforcement apparently took the first sentence, "We need to take information, wherever it is stored, make our copies and share them with the world," as the motive and purpose behind his extensive downloading—some 4.8 million articles, or 80% of JSTOR's database of journals. ("It is alleged that Swartz avoided MIT's and JSTOR's security efforts in order to distribute a significant proportion of JSTOR's archive through one or more file-sharing sites.")[14]

Collecting the JSTOR articles through the MIT network was not the first time Aaron Swartz had engaged in large-scale downloading, although it was the first time he was charged with a crime. In 2008, he downloaded about 20 million pages of documents from the government-run PACER (Public Access to Court Electronic Records) system. Unlike the JSTOR documents, these were all in the public domain.[15] "He donated the 19,856,160 pages to http://public.resource.org, an open government initiative spearheaded by Carl Malamud as part of a broader project to make public as many government databases as Malamud can find."[16] The FBI opened an investigation, but apparently concluded that no laws were violated, and thus no charges were filed.[17]

---

[12] Government's consolidated Response to Defendant's Motions to Suppress at 3, Doc. No. 81 (filed November 11, 2012), *United States v. Swartz*, Case No. 1:11-cr-10260-NMG.

[13] <http://archive.org/stream/GuerillaOpenAccessManifesto/Goamjuly2008_djvu.txt>. Aaron Swartz was not the sole author of the memo, and it is unknown whether he authored the sentences that were quoted. Quinn Norton told the Review Panel that she did the final editing of the piece, and that she does not know who the other authors were, or who contributed which part.

[14] *Supra* at 4 n.15; *see also* USAO Press Release July 19, 2011, <http://www.justice.gov/usao/ma/news/2011/July/SwartzAaronPR.html>

[15] John Schwartz, "An Effort to Upgrade a Court Archive System to Free and Easy," February 12, 2009, *New York Times*, <http://www.nytimes.com/2009/02/13/us/13records.html?_r=0>.

[16] <http://www.wired.com/threatlevel/2009/10/swartz-fbi/>

[17] Aaron Swartz, together with public-domain advocate Carl Malamud, identified numerous instances of personal identifying information that was supposed to be redacted or hidden in these public documents that had been left available for viewing: "names of minor children, names of informants, medical records, mental health records, financial records, tens of thousands of social security numbers." They then sent their results to 31 district courts. The federal Judicial Conference eventually changed its privacy rules. See the comments by Public.Resource.Org Director Carl Malamud, in his January 23, 2013, memorial "Aaron's Army."

Aaron Swartz also participated in a study of downloaded articles concerning the payment by interested organizations to experts, including law professors, to publish papers in academic journals. He wrote a script that downloaded articles from Westlaw, and a second script that extracted the relevant information about the funding sources from the footnotes of each article.[18] This has been cited as support for a different possible motive for his actions: an intention to cross-reference the entire JSTOR database by author, publisher, and funding source, so as to demonstrate the extent to which JSTOR's service, and thus the fees it charged, was enabled and funded by public money.[19] In support of this interpretation is Aaron Swartz's self-description on the first page of his blog: "He [Aaron Swartz] is a frequent television commentator and the author of numerous articles on a variety of topics, especially the corrupting influence of big money on institutions including nonprofits, the media, politics, and public opinion. From 2010–2011, he researched these topics as a Fellow at the Harvard Ethics Center Lab on Institutional Corruption."[20]

One can also speculate that Aaron Swartz had not decided what he would eventually do with the articles at the time of the downloading.[21]

---

[18] S. Barday, *Punitive Damages, Remunerated Research, and the Legal Profession*, 61 *Stanford L.R.* 711 (2008). Aaron Swartz's name does not appear in this publication, but Professor Lawrence Lessig, now the Roy L. Furman Professor of Law and Leadership at Harvard Law School, and who at the relevant time was a Professor of Law at Stanford University, told the Review Panel that Ms. Barday did this study for a seminar he was teaching at Stanford Law School, and that he suggested that she and Swartz work together. Aaron Swartz and Ms. Barday collaborated on research for the piece, downloading the articles using Ms. Barday's user ID. "The database was compiled using Python source code extracting all entries contained in the Westlaw "Journals and Law Reviews" database, including full-text articles. The first three footnotes and the Westlaw "cite as" field were then extracted from the articles. Articles receiving outside funding were identified using . . . search terms as they appear in one of the first three footnotes in each article." We note that one of the articles cited in this study was authored by Review Panel member Peter A. Diamond.

[19] Lawrence Lessig in "Aaron's Laws—Law and Justice in a Digital Age," <http://www.youtube.com/watch?v=9HAw1i4gOU4&feature=player_embedded>; Quinn Norton, "Life Inside the Aaron Swartz Investigation," *The Atlantic*, March 3, 2013, <http://www.theatlantic.com/technology/archive/2013/03/life-inside-the-aaron-swartz-investigation/273654/>. On the other hand, the Review Panel notes that JSTOR provides a service, JSTOR Data for Research <http://dfr.jstor.org>, that researchers can access (including for downloading) to obtain some of the information for such a study.

[20] <http://www.aaronsw.com/>.

[21] Carl Malamud, in his memorial to Aaron Swartz, writes, "I'm convinced that Aaron had not made a decision to release those articles, and I am certain he would not have released them without a great deal of post-download analysis." (Aaron's Army: On Crime and Access to Knowledge," <https://public.resource.org/crime/pamphlet.pdf>). Or, as his friend Quinn Norton told the Review Panel, "He liked to collect data sets." Norton also told the Review Panel that Swartz was shocked by the arrest: he didn't regard what he'd done as a big deal and was surprised that people were making so much of it. His (third) attorney Elliot Peters also told the Review Panel that Swartz had been shocked by the arrest.

II.B The Prosecutions and the Legal Defense: An Overview

There were two criminal prosecutions of Aaron Swartz. The federal prosecution by the U.S. Attorney's Office (USAO) in Boston began with an indictment in July 2011, and there was a superseding indictment in September 2012. The state prosecution by the District Attorney's Office for Middlesex County ("the DA's Office") began in November 2011, and was dismissed in March 2012 by motion of the DA's Office. We discuss the state prosecution first, in section II.B.1, before turning to the federal prosecution in section II.B.2.

An overview chronology of the key legal events described in this section is as follows:

January 5, 2011	Federal criminal investigation opened
January 6, 2011	Aaron Swartz arrested
June 3, 2011	Aaron Swartz signs settlement agreement with JSTOR
July 14, 2011	Federal indictment returned by grand jury
July 19, 2011	Indictment unsealed; Aaron Swartz arraigned in federal court
November 6, 2011	State indictment issued
September 12, 2012	Superseding federal indictment returned
October 5, 2012	Defense files motions to suppress evidence
November 16, 2012	Government files opposition to motions to suppress
March 8, 2012	State charges dismissed

During the time between his arrest on January 6, 2011, and his death on January 11, 2013, Aaron Swartz was represented in these criminal matters, at separate times, by three sets of attorneys, as well as a fourth attorney who overlapped the first two. Aaron Swartz's father, Robert Swartz, was also active in the defense.

The first law firm representing Aaron Swartz was Good & Cormier, in Boston.[22] Mr. Andrew Good was Aaron Swartz's lead counsel. The firm represented Swartz in the

[22] This firm had previously represented Aaron Swartz during a criminal investigation conducted by the FBI, in Boston, regarding the downloading of court documents from the Public Access to Court Electronic Records (PACER) system. There are no copyrights in court records, and the downloading took place during a period of time when, and at a location where, PACER was not charging for downloading. The FBI investigation concluded with no prosecution of Aaron Swartz or of anyone else.

federal case and was involved from the day of Swartz's arrest until the fall of 2011, after the first federal indictment was handed up but before the state indictment was issued and subsequently dismissed.

The second firm was that of Martin G. Weinberg, Esq., also in Boston. Mr. Weinberg assumed the representation from Good & Cormier beginning in the fall of 2011, and continued until the end of October 2012, after the federal superseding indictment was handed up. It was during this time period that the state case was indicted and then dismissed.

The third firm was Keker & Van Nest LLP, in San Francisco. Mr. Elliot Peters was Aaron Swartz's lead counsel. This firm took over the representation from Martin Weinberg and continued until Aaron Swartz's death on January 11, 2013.

William Kettlewell of Collora LLP (in Boston) was also involved in the defense, during a period overlapping the involvement of Good & Cormier and Martin Weinberg. Neither Mr. Kettlewell nor his law firm appeared in court in either the federal or state case.[23]

II.B.1 The state prosecution

Upon his arrest, Aaron Swartz was charged in Cambridge District Court with two felonies of breaking and entering in the daytime: one count each for January 4 and January 6, 2011.

On November 6, 2011, after the initial federal indictment was handed up, the DA's Office obtained a state indictment against Aaron Swartz charging him with six felony counts: two counts of breaking and entering a building (at MIT) with the intent to commit a felony; three counts of accessing a computer without authorization; and one count of larceny—stealing the electronically processed or stored data of JSTOR—in an amount over $250. This indictment was handed up not in Cambridge District Court but rather in a different court: the Superior Court for Middlesex County.[24]

MIT was not involved in the state prosecution. It first learned of the prosecution on November 17, 2011, through a Cambridge DA's Office press release.[25] MIT was not

---

[23] Throughout the relevant period, MIT's Office of the General Counsel was under the impression that Mr. Kettlewell represented Robert Swartz rather than Aaron Swartz. However, Mr. Kettlewell clarified this during his interview with the Review Panel.

[24] According to attorneys for Aaron Swartz, prosecutions in Superior Court are normally used for more serious cases; the sentences handed down in this court are typically harsher than those handed down in District Court; and it is more difficult to resolve a case in Superior Court without an adjudication or without jail time than in District Court.

[25] "Cambridge Man Indicted On Breaking & Entering Charges, Larceny Charges in Connection With Data Theft", <http://middlesexda.com/news/press-release-archive.php?reference=456>.

asked to provide documents, to produce witnesses to be interviewed, or to testify. MIT did not seek to press charges, and did not intervene or lobby to have the charges dismissed.

After the state indictment, Martin Weinberg filed demands for discovery. In state prosecutions that involve joint investigations with outside law enforcement agencies or foreign jurisdictions, Massachusetts state law governing criminal discovery requires that the District Attorney obtain from those agencies and jurisdictions certain evidence that may be relevant to the case. Some of this evidence was in the sole possession of the Boston U.S. Attorney's Office and the U.S. Secret Service. Mr. Weinberg demanded this material as discovery from the DA's Office, and the USAO refused to produce it to that office. As a result, the DA's Office could not comply with the Massachusetts discovery laws so as to continue its prosecution, and it dismissed its charges.

II.B.2 The federal prosecution

The U.S. Attorney's Office opened its criminal investigation on January 5, 2011.[26] Assistant U.S. Attorney (AUSA) Stephen Heymann, head of the Internet and Computer Crimes Unit within the USAO, directed the investigation and eventual prosecution. (Stephen Heymann is referred to as "the lead prosecutor" throughout the rest of this report.) Shortly after Aaron Swartz's arrest, the lead prosecutor and the special agent who had been at MIT on January 4 spoke with and interviewed personnel from IS&T and the MIT Police. Eventually two grand jury subpoenas for documents were served upon MIT.[27] More will be said about these subpoenas, and MIT's response to them, in Part III.

The initial indictment was handed up by a federal grand jury, sitting in Boston, on July 14, 2011. It charged Aaron Swartz on four felony counts, these being one count of wire fraud and three counts of violating the Computer Fraud and Abuse Act (CFAA).[28] Each

---

[26] On this day the Secret Service special agent sent an email to an Assistant U.S. Attorney in Boston inquiring about the statutes that might be used to prosecute the person involved. The U.S. Department of Justice can begin a criminal investigation without knowing the identity of the perpetrator who engaged in the conduct under investigation. In such circumstances, the matter is opened for an "UNSUB," indicating an unknown subject.

[27] An initial and then a superseding indictment were returned by grand juries sitting in Boston, separated in time by about fourteen months. They were signed by different foremen. For these reasons we assume that the indictments were considered and returned by different grand juries. Both subpoenas appear to have been issued by the first of these grand juries.

[28] 18 U.S.C. §1030 criminalizes various forms of conduct pertaining to "protected computers," which include computers used in or affecting interstate commerce, among these, any computer connected to the Internet. The forms of conduct that are made illegal by this Act include those involving: accessing a computer without authorization or exceeding authorized access; accessing a computer with intent to defraud; and transmitting information that results in damage. The first indictment charged Aaron Swartz (count three) with both (a) accessing protected computers (the MIT network and JSTOR's computer system) without authorization and (b) exceeding authorized access. The superseding indictment, although

of the three latter counts is based upon a different legal theory.[29] At no time had the U.S. Attorney's Office sought the permission, opinion, or support of MIT for this prosecution before the indictment was handed up. MIT learned of the indictment for the first time on the day it was unsealed (July 19) through a phone call from the prosecutor to an attorney in OGC.

Andrew Good was notified by the U.S. Attorney's Office on July 18 (Monday) about the indictment, and he arranged to have Aaron Swartz voluntarily appear for his initial court appearance on the early morning of July 19. Following the normal procedures of the U.S. Marshal's Service, Aaron Swartz was arrested on the federal charges.[30] He was held in lockup pending his being interviewed by Pretrial Services and was otherwise processed (including the taking of biographical information and fingerprints by the U.S. Marshals Service).

On the day of his arrest, Aaron Swartz issued 11 tweets from his Twitter account, most referencing the website of Demand Progress, which published an article about Aaron Swartz's indictment and arrest and solicited statements of support for him.[31] Demand

---

increasing the number of counts from four to 13, removed the accusation that Aaron Swartz exceeded authorized access, while keeping the charge that he accessed the computers without authorization. More detail as to the legal theories for each count in the initial complaint is provided in the next footnote.

[29] Count one charged Aaron Swartz with defrauding JSTOR of property, that is, "journal articles digitized and distributed by JSTOR, and copies thereof," by use of a wire transmission, in violation of 18 U.S.C. § 1343. Count two charged Aaron Swartz with accessing a protected computer (on the MIT and the JSTOR networks) without authorization and also in excess of authorized access, with the intent to defraud and obtain things of value, these being "digitized journal articles from JSTOR's archives." This was in violation of 18 U.S.C. § 1030(a)(4). Count three charged him with intentionally accessing a computer (on the MIT and the JSTOR network) without authorization and in excess of authorized access, and thereby obtaining information having a value in excess of $5,000. This was in violation of 18 U.S.C. § 1030(a)(2), (c)(2)(B)(iii). Count four charged Aaron Swartz with intentionally accessing, without authorization, a protected computer (on the MIT and the JSTOR network), in a manner affecting at least 10 computers, and as a result of such conduct causing damage in excess of $5,000. This was in violation of 18 U.S.C. § 1030(a)(5)(B), (c)(4)(A)(i)(I) and (VI). All counts were felony charges.

The indictments also alleged that Aaron Swartz aided and abetted someone else in committing these criminal offenses; however, nowhere in the indictments is such other person identified, described, or otherwise alluded to, and the Review Panel has learned of no basis for this allegation.

[30] The prior arrest in Cambridge on January 6 was on the state charges.

[31] "Federal Government Indicts Former Demand Progress Executive Director for Downloading Too Many Journal Articles," <http://web.archive.org/web/20110721132939/http:/blog.demandprogress.org/2011/07/federal-government-indicts-former-demand-progress-executive-director-for-downloading-too-many-journal-articles/>. The Director of Demand Progress, together with Aaron Swartz's friend Quinn Norton, wrote the article while Swartz was in custody.

Progress also embarked on a petition drive in his support. The Demand Progress website later indicated that more than 35,000 people had signed the petition.[32]

A superseding indictment was returned by a second grand jury, also sitting in Boston, on September 12, 2012 (14 months after the initial indictment). It charged Aaron Swartz with 13 felony counts, these being two counts of wire fraud and 11 counts of violating the CFAA. Essentially, the superseding indictment took the four counts from the initial indictment and broke each of them into multiple counts, by charging Aaron Swartz's alleged conduct (as related to each of the four legal theories of liability) as discrete events in place of being merged into single allegations of liability. Also, the theory of liability for the final count, alleging damage to a protected computer, was expanded.[33]

II.B.3 Plea discussions during the federal prosecution

The USAO and Aaron Swartz's defense team held plea discussions during 2011 and 2012. The key issues discussed were: (a) whether Aaron Swartz would have to plead guilty to a felony; (b) whether he would need to serve jail time, and if so, how much.

---

[32] "More than 35,000 Sign Petition In Support of Aaron Swartz," <http://web.archive.org/web/20110723204917/http://blog.demandprogress.org/2011/07/more-than-35000-sign-petition-in-support-of-aaron-swartz/>.

[33] One effect of these charging decisions was to—theoretically—increase the maximum penalties to which Aaron Swartz might be subject from 35 years to 95 years imprisonment; and from $1 million to $3 million in fines. We note that, as a practical matter, the U.S. Sentencing Commission Guidelines take into account the relevant conduct of a person convicted of a crime, giving little regard to the number of counts for which that person is convicted. A judge is not obligated to follow the sentencing guidelines—but must explain on a sentencing form—that is, on the record—why the court has "departed" from the guidelines.

It is legally proper to include (or "bundle") two or more events as part of a single count in an initial indictment, even where each event is chargeable as a separate crime as defined by a single criminal statute. It is also proper to treat such separate events as separate crimes or counts in such an indictment. Thus, while not legally required, it is appropriate to charge multiple events in one count; similarly, although not legally required, it is appropriate to charge such multiple events in multiple counts.

We also note that the U.S. Attorneys' Manual (USAM), published by the U.S. Department of Justice and establishing policy for all U.S. Attorneys' Offices, contains the following comment regarding charging decisions:

Comment: It is important to the fair and efficient administration of justice in the Federal system that the government bring as few charges as are necessary to ensure that justice is done. The bringing of unnecessary charges not only complicates and prolongs trials, it constitutes an excessive—and potentially unfair—exercise of power. To ensure appropriately limited exercises of the charging power, USAM 9-27.320 outlines three general situations in which additional charges may be brought: (1) when necessary adequately to reflect the nature and extent of the criminal conduct involved; (2) when necessary to provide the basis for an appropriate sentence under all the circumstances of the case; and (3) when an additional charge or charges would significantly strengthen the case against the defendant or a codefendant. "Additional Charges," USAM 9-27.320 B.

See also United States v. Goodwin, 457 U.S. 368 (1982) (discussing appropriateness of seeking additional charges in a superseding indictment prior to trial).

According to the USAO, the earliest plea offer made to Aaron Swartz was the following: "a plea of guilty to a single felony count with a recommended sentence of three months imprisonment, to be followed by a period of supervised release the conditions of which included a period in a halfway house, a period of home confinement, and—as is common in computer crime cases—restrictions on his use of computers during the period" of supervision.[34]

According to Andrew Good, the first plea offer made by the U.S. Attorney's Office came from the lead prosecutor before the initial indictment was returned. It included the following: Aaron Swartz would plead guilty to a felony; he would serve 13 months imprisonment; a period of supervisory release would follow the incarceration;[35] and restrictions would be placed on Aaron Swartz's computer use during the supervisory release. Aaron Swartz rejected this plea offer. According to Mr. Kettlewell, during a pre-indictment meeting with at the USAO, a plea offer of six months imprisonment was made. It was rejected.

During the negotiations that followed this rejection, the USAO offered periods of jail time of up to six months, which included additional restrictions similar to the ones already discussed. That is, offers involved a "split sentence" (under which a defendant serves a term of imprisonment followed by a period of community confinement or home detention).

According to the U.S. Attorney's Office, there was a period of time after the indictment when the government offered a plea along the following lines: Aaron Swartz would plead guilty; the government would retain the option to ask for jail time of up to six months; and the defense would be free to argue for a no-jail, probationary sentence. Martin Weinberg and Robert Swartz offered the following clarification of this offer for the Review Panel: Aaron Swartz would have to plead guilty to all four felony counts of the initial indictment; and a period of supervised release would follow any period of incarceration.

According to Mr. Weinberg, an alternative plea offer, extended about the same time, would have required Aaron Swartz to waive his right to argue for no jail time, but would have reduced the time sought by the government to four months or less. Both plea offers could have been subject to further negotiations;[36] however, they were rejected by the

---

[34] Letter from the USAO to the Review Panel.

[35] Supervisory release is a form of probation that follows incarceration.

[36] According to Mr. Weinberg, items that might have been open to further negotiations included the number of counts of the initial indictment to which Aaron Swartz would have been required to plead guilty.

defense because—under the scope for such negotiations permitted by the USAO—under no circumstances could Aaron Swartz obtain a guarantee of no jail time.[37]

According to Aaron Swartz's attorneys, at no time did federal prosecutors entertain a plea agreement for him that assured him no jail time,[38] and the prosecutors always insisted on a plea to a felony as opposed to a lesser charge, that is, to a misdemeanor.[39] It was during these discussions, according to Andrew Good, that he informed the lead prosecutor that Aaron Swartz was suicide risk, and the prosecutor responded that the office could have him locked up (presumably to prevent such an occurrence).

All of these negotiations occurred against the backdrop of the U.S. Sentencing Commission Guidelines, which—although not binding upon federal judges—provide a calculus for a judge to use in determining the appropriate sentence for a defendant. Among the more significant factors under the guidelines is the value of property sought to be taken by the perpetrator of a crime, including crimes defined by the Computer Fraud and Abuse Act. We note that this is the value of the property *sought to be taken*, and not of property *actually* taken. Given the allegations in each of the two indictments, and the evidence the government intended to introduce at trial concerning the value of the JSTOR articles Aaron Swartz sought to download, he was realistically facing a sentence calculated under the guidelines of some seven years incarceration plus supervisory release and fines in the event of conviction at trial and in the absence of any plea agreement.[40]

MIT was never involved in any plea negotiation, and was never asked—by either the prosecution or the defense—to approve or disapprove any plea agreement.

---

[37] Rule 11(c)(1)(C) of the Federal Rules of Criminal Procedure provides that where the government and a defendant agree that a specific sentence or sentencing range is the appropriate disposition of the case, such recommendation or request binds the court once the court accepts the plea agreement. As the government never agreed to a guarantee of a disposition of this case with no jail time, this rule was not available to Aaron Swartz for the purpose of withdrawing his plea of guilty in the event that the sentencing judge chose to impose jail time as part of the sentence.

[38] Confirmation was provided by JSTOR's outside counsel at Debevoise & Plimpton LLP, by Robert Swartz, and by Quinn Norton.

[39] Confirmation provided by Robert Swartz and Quinn Norton.

[40] At the time of Aaron Swartz's indictment, the USAO stated: "If convicted on these charges, Swartz faces up to 35 years in prison, to be followed by three years of supervised release, restitution, forfeiture and a fine of up to $1 million." *See* USAO Press Release July 19, 2011, <http://www.justice.gov/usao/ma/news/2011/July/SwartzAaronPR.html>

II.B.4 Motions to suppress

On October 5, 2012, Attorney Weinberg, on behalf of Aaron Swartz, filed five motions to suppress evidence and one motion to dismiss the indictment.[41] Among the arguments made in these motions to suppress was that the government and MIT had violated the Stored Electronic Communications Act; violated Swartz's Constitutional right under the Fourth Amendment against unreasonable search and seizure; and violated his expectation of privacy under MIT's policy concerning the maintenance and routine destruction of computer records (specifically, the DHCP logs). The government filed its opposition on November 16, 2012.

II.C Aaron Swartz's Settlement with JSTOR

Early in 2011, shortly after the arrest of Aaron Swartz, attorneys at Good & Cormier engaged in a strategy of trying to convince the USAO that no prosecution should be pursued; and, failing this goal, to convince it that an agreement with no felony conviction and no jail time was appropriate for resolving the matter. As part of this strategy, the firm sought to obtain JSTOR's support for such a resolution.

JSTOR had an inside general counsel. It also used outside counsel from the New York law firm Debevoise & Plimpton, LLP. When the USAO began asking for information from JSTOR as part of the grand jury's investigation, JSTOR asked the USAO to issue a subpoena for the information, and the USAO complied. While collecting information necessary for complying with the subpoena, it examined its internal records and determined the following: the "third" episode of downloading, which it discovered on December 26, 2010, had actually begun in late November. The stream of requests that instigated these downloads was structured in such a way that none of the triggers JSTOR had inserted into its systems to warn it of any such renewed downloading had reacted. JSTOR finally determined that Aaron Swartz had obtained some 4.3 million articles (these were in addition to the 450,000 articles downloaded in the September and October incidents).

JSTOR was extremely concerned about the status of the data that Aaron Swartz had downloaded: the material might be placed on the Internet and widely disseminated from there. JSTOR felt that this might even damage its viability, because the publishers and copyright holders of the articles it stored might no longer trust the organization.[42]

---

[41] Under the Court's scheduling order, this was the last permissible day for the filing of such motions. Of the five motions to suppress, four referred to MIT.

[42] This information was provided to the Review Panel by the president of JSTOR.

Good & Cormier spoke with JSTOR's outside counsel, seeking a civil settlement that would resolve any civil liability that Swartz might have with the company.[43] It also asked that JSTOR tell the USAO directly that it was not interested in Aaron Swartz being prosecuted or jailed. At this time, JSTOR had not filed, nor had it threated to file a civil lawsuit—although in theory it could have done so.

A civil settlement agreement with JSTOR was achieved on June 3, 2011. Aaron Swartz certified that he had not made any copies of the data that he had downloaded, and Good & Cormier delivered the only disk containing this data to the USAO. This satisfied JSTOR, as it now knew where the data was kept and that it was secure. In addition, Aaron Swartz paid over $26,500 to JSTOR, composed of $1,500 for damages and $25,000 in attorneys' fees and costs.[44]

Once this settlement agreement was signed, two outside counsel for JSTOR spoke on several occasions with the lead prosecutor, a second line prosecutor in Boston involved in the case, and a supervisory prosecutor in Boston (not the U.S. Attorney). They told these prosecutors that, although JSTOR recognized that any charging decision was entirely up to the government, JSTOR was not pressing for criminal charges and preferred, from its perspective, that no charges be brought.[45]

On July 19, 2011, the day that the federal indictment was unsealed, JSTOR issued a press release that included the following:[46]

> [W]e have been subpoenaed by the United States Attorney's Office in this case and are fully cooperating . . . .
>
> The criminal investigation and today's indictment of Mr. Swartz has been directed by the United States Attorney's Office. It was the government's decision whether to prosecute, not JSTOR's. As noted previously, our interest was in securing the content. Once this was achieved, we had no interest in this becoming an ongoing legal matter . . .

---

[43] In addition to its criminal penalties, the Computer Fraud and Abuse Act allows victims to seek compensation from persons who cause them harm through violations of the Act by bringing civil actions against such persons. *See* 18 U.S.C. § 1030(g).

[44] We note that this $1,500 of negotiated damages, by itself, is less than the $5,000 minimum in damages required to escalate CFAA charges in the two indictments from misdemeanors to felonies. More about the measurement of damages and its effect on the seriousness of the charges is discussed in Appendix 11, Comments on the Computer Fraud and Abuse Act Charges against Aaron Swartz, section II.C, Losses Exceeding Five Thousand Dollars.

[45] This information was provided to the Review Panel by JSTOR.

[46] <http://about.jstor.org/news/jstor-statement-misuse-incident-and-criminal-case>

With regard to JSTOR's involvement in the criminal prosecution, we note the following. When, on January 11, the Secret Service asked JSTOR about the value of its database, JSTOR declined to answer. Later, when the USAO contacted JSTOR for information, JSTOR insisted on being served with a subpoena. Multiple subpoenas were served, and JSTOR tried to limit the information it provided to answering subpoenas. The government did not ask JSTOR's management whether there was unauthorized access, fraud, deception, or damage.[47] Its inquiries of JSTOR prior to the indictment were "superficial."[48] No JSTOR employees were interviewed prior to the indictment[49] (although the prosecution had access to JSTOR's documents through subpoenas.)[50]

[47] This comment was provided to the Review Panel by the president of JSTOR.

[48] This comment was provided to the Review Panel by JSTOR's outside counsel.

[49] This comment was provided to the Review Panel by JSTOR's outside counsel.

[50] According to the UAO, four JSTOR employees participated in a conference call with "members of the United States' investigatory team," where one employee said that the JSTOR terms and conditions "clearly prohibited the kind of downloading" engaged in by Aaron Swartz; and a JSTOR employee was in "regular contact" with the prosecution from the beginning of the investigation and "provided information prior to the indictment." According to JSTOR's outside counsel, the indictment was returned without benefit of interviews with JSTOR personnel; the USAO began to interview JSTOR employees in December 2012, and the questioning focused on the nature of Swartz's access of JSTOR's network but it did not ask explicitly about gaining unauthorized access or exceeding authorized access..

Part III: MIT'S RESPONSE TO THE PROSECUTION (January 2011–January 2013)

The prosecution of Aaron Swartz lasted just over two years and ended at the time of his suicide on January 11, 2013. During this time MIT's administration and its Office of the General Counsel (OGC) interacted with (among others) the Boston U.S. Attorney's Office, JSTOR, Aaron Swartz's defense attorneys, and Aaron Swartz's father, Robert Swartz. OGC hired outside counsel to provide it with advice regarding the criminal prosecution and to interact on its behalf with the U.S. Attorney's Office and the defense.

It produced documents and made MIT employees available for discussions and interviews with both the USAO and the defense.

MIT's Office of General Counsel was a principal participant in handling and otherwise making decisions regarding MIT's conduct as to the Swartz prosecution. OGC made its decisions in consultation with and with approval from the administration, and in consultation with some members of the faculty, including leaders of MIT's Faculty Policy Committee.[1] OGC took guidance from MIT's senior officers, and also kept MIT's Academic Council informed.

A timeline of significant events covered in this part of the Report[2] is as follows:

No.	Date	Event
1	January 4, 2011	Laptop doing the JSTOR downloading is found.
2	January 5, 2011	U.S. Attorney's Office opens criminal investigation of the accessing of MIT's network.[3]
3	January 6, 2011	Aaron Swartz is arrested.
4	January 27, 2011	First grand jury subpoena is served on MIT.
5	May 6, 2011	The lead prosecutor tells OGC that Aaron Swartz rejected a plea offer and the case would likely move forward as a felony charge.
6	June 3, 2011	JSTOR settles its possible civil claims with Aaron Swartz.
7	June 6, 2011	MIT retains outside counsel experienced in criminal law.

[1] MIT's senior officers include the President, Provost, Chancellor, Executive Vice President, and Vice President and Secretary of the Corporation. Over the period covered by this section of the Report, OGC dealt with two presidents, two provosts, two executive vice presidents, and two chancellors. MIT's Academic Council includes the senior officers, deans, vice presidents, and the Director of Libraries.

[2] See Appendix 5 for a more comprehensive timeline.

[3] A criminal investigation of possible criminal conduct may be opened by a U.S. Attorney's Office upon request of a federal law enforcement agency without the identity of the perceived perpetrator or any suspect being known. In such circumstances the file is opened under the name of an "Unknown Suspect," or an "UNSUB." Also, federal law enforcement agencies, such as the U.S. Secret Service, can open their own criminal investigations. These may be separate from although not necessarily independent from those of a U.S. Attorney's Office.

8	June 13, 2011	Robert Swartz reaches out to the incoming Director of the MIT Media Lab, where he is a consultant, for assistance in dealing with MIT's administration and its Office of the General Counsel on behalf of his son.
9	June 13, 2011	OGC sends email to defense attorney William Kettlewell, informing him that MIT is not taking a position on whether Swartz should be prosecuted.
10	June 21, 2011	A conversation with the lead prosecutor leads OGC to infer that MIT's views on the case will have little impact on the prosecution going forward.
11	June 24, 2011	Second grand jury subpoena is served on MIT.
12	July 14, 2011	Federal indictment is returned and sealed.
13	July 19, 2011	Aaron Swartz voluntarily appears at the federal courthouse and is arrested.
14	July 19, 2011	The federal indictment is unsealed.
15	July 19, 2011	JSTOR issues a public statement disclaiming interest in further prosecution.
16	July 19, 2011	Demand Progress publishes article on Internet and solicits statements and signatures in support of Aaron Swartz.
17	September 14, 2011	Robert Swartz meets with MIT's Chancellor and an attorney from the OGC, and is told MIT's position is that of "neutrality."
18	October 25, 2011	Martin Weinberg takes over as Aaron Swartz's new defense attorney.
19	October 27, 2011	Andrew Good withdraws as defense attorney for Aaron Swartz.
20	April 25, 2012	William Kettlewell and Martin Weinberg meet with MIT's outside counsel.

21	August 9, 2012	MIT's outside counsel speaks with the lead prosecutor, communicating MIT's positions on various issues concerning the prosecution of Aaron Swartz.
22	September 12, 2012	Robert Swartz again meets with MIT's Chancellor and an attorney from the OGC.
23	September 12, 2012	Superseding indictment is returned by a federal grand jury.
24	September 18, 2012	Two Assistant U.S. Attorneys, the U.S. Secret Service Special agent, and the detective from the Cambridge Police Department meet with and interview several MIT employees.
25	September 28, 2012	Martin Weinberg and William Kettlewell meet with MIT's Chancellor, General Counsel, and outside counsel, asking MIT to meet with the USAO in support of Aaron Swartz, and describing the motions they will file to suppress evidence, including that the motions will allege that MIT collected or produced information unlawfully.
26	October 5, 2012	Martin Weinberg files five motions to suppress evidence and one motion to dismiss the indictment.
27	October 16, 2012	Two MIT employees from IS&T are interviewed by two Assistant U.S. Attorneys and a Cambridge Police detective.
28	October 26, 2012	MIT's outside counsel notifies Martin Weinberg that MIT is willing to accompany the defense to a meeting with the U.S. Attorney's Office and of what MIT is willing to say, and not willing to say.
29	October 31, 2012	Martin Weinberg withdraws as Aaron Swartz's defense attorney.
30	November 6, 2012	Elliot Peters notifies MIT's outside counsel that Aaron Swartz's defense no longer seeks its participation in a meeting with the U.S. Attorney's Office.

31	November 8, 2012	Elliot Peters and Michael J. Pineault assume representation of Aaron Swartz in federal court.
32	November 30, 2012	MIT receives a subpoena from Aaron Swartz's attorneys seeking documents.
33	December 11, 2012	Two MIT employees, one from MIT Libraries and one from IS&T, are interviewed by an attorney and an expert witness for Aaron Swartz.
34	December 14, 2012	A hearing on the previously filed motions to dismiss and suppress is scheduled for January 25, 2013.
35	January 11, 2013	Aaron Swartz, age 26, commits suicide in Brooklyn, New York.

III.A Events between the Arrest and the Indictment (January 2011–July 2011)

Apart from providing information to the prosecution and responding to grand jury subpoenas, matters remained quiet for MIT during the period between the January 6 arrest of Aaron Swartz and mid-June, a month or so before his indictment. Initially, MIT's Office of the General Counsel did not know the background of Aaron Swartz. A few days after the arrest OGC did a search on his name on the Internet and learned about him and his background.

During the early post-arrest period, MIT was involved in three matters concerning Aaron Swartz: (1) responding to requests by the prosecution for documents and information about Swartz's conduct on the MIT network; (2) developing and implementing a position of neutrality; and (3) discussing with JSTOR the possibility of making a joint public statement on the Swartz matter. Significant communications between MIT and Aaron Swartz's attorneys and his father, Robert Swartz, did not begin until June 2011.

III.A.1 MIT provides information to the USAO (January 2011–April 2011)

In the time between the discovery of the laptop in the basement closet on January 4 and the arrest of Aaron Swartz on January 6, IS&T, after consultation with OGC, provided documents to the Secret Service, doing so without MIT having been served with a subpoena, as noted in section I.B.[4] During this period, OGC was primarily concerned with avoiding disclosure of "personal identifying information," rather than the requirements of wiretap laws that might be applicable to the investigation.

MIT cooperated with law enforcement beginning with their arrival on campus. Specifically, there were interactions with a federal prosecutor, a Secret Service special agent, and a detective from the Cambridge Police Department.[5] These officials acted as a team for the purposes of seeking information from MIT and otherwise conducting the post-arrest investigation. The USAO asked for the preservation of relevant evidence, and consistent with its general practice in other cases OGC agreed to preserve it. OGC helped to schedule interviews, which took place in the OGC offices, with employees from IS&T and the MIT Libraries. Brought to these meetings were additional relevant documents for the purpose of refreshing the memories of the persons interviewed. OGC set ground rules stipulating that the investigators could continue to talk directly to the witnesses they had already interviewed, without OGC involvement, but for new witnesses or new areas of inquiry, OGC would want to participate.

On January 24, 2011, the Secret Service Agent asked IS&T for a copy of the packet data capture and the video surveillance file. IS&T duplicated the hard drive it had used to capture the packet stream (see section I.B), and the special agent picked up the copy at MIT on January 26.[6]

As of January 25, the USAO and the Secret Service continued to seek yet more information. On January 27, MIT was served with the first of two grand jury subpoenas: the OGC would not have agreed to provide additional material without such a subpoena. The first subpoena called for the following:

> With respect to actual and attempted excessive downloads from JSTOR between September 25, 2010, and January 6, 2011, from IP addresses assigned to buildings 16, 4, and W20, provide the following:

---

[4] These documents are the network flow data, the DHCP logs, and the RADIUS server logs, listed as items (1)-(3) of section I.B. Appendix 7 presents a more complete technical description. Appendix 10 gives the Review Panel's legal analysis of their having been turned over without subpoena.

[5] The first post-arrest email between the lead prosecutor and an attorney in the Office of MIT's General Counsel occurred on January 7, 2011. It asked for the preservation of certain evidence, essentially the same evidence that was commanded by the first grand jury subpoena served on MIT on January 27.

[6] The packet capture data is listed in section I.B item (4), and described more fully in Appendix 7. Appendix 10 comments on the legality of MIT having turned over this data.

(1) All electronic logs and records MIT has and can recover concerning the events;

(2) All non-privileged electronic mail, notes, reports, records, documents, correspondence and other materials regarding or referring to the events;

(3) All photographs, videos and other images taken by surveillance camera(s) in the utility closet in Building 16 utilized during the events;

(4) Screen shots of MIT's guest login process and any associated terms of use; and

(5) All records of expenditures of time and money to respond to the events.

In response to this subpoena, MIT made four separate productions of documents over the course of three months. The first three productions, on February 4, 18, and 28, dealt with items 1 through 4.[7] In addition to this document production, an IS&T network engineer answered, by email, questions posed by the lead prosecutor concerning MIT's network and Swartz's conduct. This began immediately after the arrest and continued throughout the prosecution.[8]

With regard to item 5, requesting records of expenditures of time and money, OGC informed the lead prosecutor shortly after receiving the subpoena that MIT normally does not keep records related to time spent by individual staff on specific tasks, and it did not believe that MIT had incurred any out-of-pocket expenses, with several trivial exceptions. When asked by the USAO, MIT provided (by letter dated April 13) an estimate of the time spent by IS&T and Libraries staff members on MIT's response to the downloading events, both before Aaron Swartz's arrest and afterwards, as well as an

[7] The requested items (1) through (4) were produced on the following dates: (a) February 4, 2011: collections of documents maintained by one employee, each, from IS&T and the MIT Libraries; (b) February 18, 2011: collections of documents maintained by three additional employees of IS&T, and printouts of various screen shots relating to MIT's guest login process; and (c) February 28, 2011: a collection of documents maintained by yet another employee of IS&T.

[8] In addition, in mid-February, the lead prosecutor wrote to OGC inquiring whether OGC could accept a subpoena demanding logs from a computer belonging to the Student Information Processing Board (SIPB), a student organization. OGC consulted with a student official of SIPB, and concluded that the logs were not likely to provide the information that the prosecutor desired. In response to the written inquiry, OGC and SIPB provided some basic information about the machine. No other additional information was provided, and the subpoena was never served.

estimated hourly dollar figure for each employee.[9] The salary payments to the employees would have been incurred regardless of the Swartz incident.

III.A.2 MIT is informed about the prosecution (March 2011–June 2011)

Sometime in mid-March, the lead prosecutor informed OGC by telephone that the USAO had taken investigative steps that would serve to put the primary suspect on notice that an investigation was ongoing. This was how MIT learned that the government was actively moving to prosecute Aaron Swartz.[10] During this conversation, the lead prosecutor also said that proving the required "jurisdictional amount" for prosecution ($5,000 or more) would not be difficult because of what had been done to JSTOR.

On May 6, the lead prosecutor asked OGC for all of the data so far provided by MIT in paper format to be reproduced in native digital format.[11] OGC refused because of the time and expense that would be required to comply. Instead, as a compromise, MIT scanned all the documents and placed them on a CD.

During the same conversation, the lead prosecutor gave an update on the prosecution: He stated that discussions with Swartz had gone nowhere, and that Swartz was not interested in any deals. He also stated that the prosecution was likely moving forward with seeking an indictment. Finally, he communicated the terms of the plea deal he had offered: If the JSTOR documents were not disseminated by Swartz, and Swartz provided an affidavit to that effect, then the prosecution would allow him to plead guilty to one felony count and "recommend a sentence below the guidelines."

On June 21, 2011, the lead prosecutor called MIT to request information on the journals and databases to which the MIT Libraries subscribed. OGC did not consider the first subpoena to cover this material, and requested a second subpoena.[12] MIT received this second subpoena by facsimile on June 24, 2011, asking for: "Documents sufficient to

---

[9] MIT applied hourly rates as follows: (a) for the IS&T personnel, it applied rates used to estimate software development costs; and (b) for the personnel with MIT Libraries, it used actual salary and benefits to calculate an hourly rate. In this letter, MIT informed the prosecutor that for some of the individuals listed, identified by name, the relevant time expended by them occurred after law enforcement became involved. Although this calculation was not made in the letter, applying the estimated hours to the hourly rates would have resulted in a figure of $10,104.75. The portion of this amount incurred before the arrest was under $3,500. The remaining time, and its estimated value, was incurred responding to the prosecution's requests for documents and information after the arrest of Aaron Swartz.

[10] About this time, the U.S. Secret Service executed several search warrants at locations frequented by Aaron Swartz, seeking computer equipment and downloaded data.

[11] "Native" format means the format used to encode data by a program or application. Without access to that program or application data may not be readable.

[12] The lead prosecutor called to ask for the journal and database information, using the initial subpoena as the legal grounds for doing so. The initial subpoena was very broad, and the information sought by the lead prosecutor in this phone call could be read to fall within its scope. OGC, however, read the subpoena conservatively and would not produce the additional material without the second subpoena.

show all journals and databases to which the MIT libraries subscribed between September 1, 2010 and July 6, 2011." MIT responded on July 6, 2011.[13]

During the June 21 conversation, the lead prosecutor also told OGC that, essentially, his work was done, that the final decision about the prosecution was now in the hands of his supervisors, and that a decision would be made soon. The OGC attorney took the opportunity to suggest that some people at MIT would be likely to view the prosecution negatively. The lead prosecutor replied that he understood the complex dynamics at MIT. He said that he had also been in touch with JSTOR and understood their perspective, and had taken both into account in moving forward with the prosecution and he would let MIT know when the indictment came down. From this, OGC inferred that further presentations of MIT's opinions were unlikely to have an effect on the prosecution: the views of both potential victims had already been taken into account. JSTOR (at that point) was regarded as the primary victim, and if JSTOR's view didn't have an impact, then neither would MIT's view.

III.A.3 MIT adopts and maintains a posture of neutrality

Very early in this post-arrest period, MIT decided to "remain neutral," as between the government and Aaron Swartz, in the investigation and eventual prosecution. Initially this meant simply that MIT would not take a public position on the prosecution. Throughout the following (almost) two years, MIT's decisions were mostly guided by this posture of neutrality. To help readers better understand the reasons for MIT's actions and decisions, we here describe the neutrality position and its evolution, before returning to the chronology of events.

In coming to assume the stance of neutrality, OGC considered that Aaron Swartz was not, and had never been, an MIT enrolled student; nor was he ever a faculty member or employee. If he had been a student, there could have been involvement of additional MIT personnel, such as faculty advisers and deans, and a possible referral to the MIT Committee on Discipline. The involvement of the disciplinary committee could have opened the way for MIT to lobby against a prosecution, in favor of its own internal resolution of an "internal" matter.[14]

---

[13] On December 12, 2012, the lead prosecutor sought yet additional documentary information from MIT, indicating that he would follow up these requests with subpoenas. At this stage of the prosecution, such subpoenas could not be issued by a grand jury but only by the Court (essentially by the prosecutor, as attorney for one of the parties and therefore as an officer of the court) pursuant to Federal Rule of Criminal Procedure 17(c), seeking documents for use at trial or another evidentiary hearing ancillary to trial, such as a suppression hearing.

[14] MIT might have adopted a neutral position even if Swartz *had been* a member of the MIT community. The cases of David LaMacchia and Andrew Huang, described in Appendix 9, show MIT adopting a neutral position with respect to the legal troubles of enrolled students.

MIT's neutrality position had two dimensions:

1. With regard to substance, MIT would make no statements, whether in support or in opposition, about the government's decision to prosecute Aaron Swartz, the government's decisions about charges in an indictment, or any possible plea bargain stances of the prosecution or the defense.[15]

2. With regard to legal procedure, MIT would treat both federal law enforcement and Aaron Swartz's defense team similarly for the purpose of providing documents and making employees available for interviews.

In adhering to neutrality with regard to substance, MIT made no public statements about the decision to prosecute, about the charges in the federal indictments, or about the state prosecution. MIT did make private statements, conveying its "neutrality" position to both prosecution and defense. These statements were meant to convey that MIT took no stand on whether there should be prosecution. Similarly, while MIT was not seeking a felony charge, neither was it opposing one. And MIT took no position on any proposed plea bargains. MIT maintained this neutrality position in its response to requests to make public statements or to intercede with the prosecution on behalf of Aaron Swartz (see sections III.B.1, III.B.4, III.C.4, III.C.5, III.D.1). In each case, MIT was willing to say that it was not advocating prosecution or jail.

Neutrality with regard to substance can be readily satisfied by making no statements. Neutrality with regard to legal procedure is more complex, and the term may be interpreted in different ways by different observers.[16] The complexity arises substantially from the differences in legal powers of the prosecution and the defense at different stages of the investigation and prosecution (see Appendix 13 on the criminal process). For example, one can respond similarly to requests for information from prosecution and defense. But in a situation where the prosecution has subpoena power and the defense does not, responding similarly does not ensure similar outcomes in the information each side actually obtains. OGC interpreted "neutrality" primarily in terms of similar responses to requests. While MIT did not conform precisely to this rule, in this sense of similar responses MIT—broadly speaking—did not side with the prosecution, nor did it side with the defense. In consequence of the differences in the powers, timing, and goals of the two parties in the case, neutrality in responses was not consistent with neutrality in outcomes, and MIT was not neutral in outcomes.

---

[15] This position of neutrality would not have necessarily extended to the sentencing phase of the prosecution, where MIT might have been prepared to advocate on behalf of Aaron Swartz had he been convicted.

[16] Such a difference in interpretation figured in Robert Swartz's disagreement with MIT's Chancellor and General Counsel over whether MIT was being "neutral." (See section III.C.4.)

In addition to adopting a position of neutrality, MIT limited its involvement, being involved only to the extent needed to respond to prosecution and defense in accord with its neutrality position. MIT had not pressed for criminal charges against Aaron Swartz; the USAO had in fact not asked MIT whether it wanted him to be prosecuted. In the words of MIT's General Counsel, "MIT viewed *U.S. v. Swartz* as exactly what the case name implies: a legal proceeding between the government and Swartz . . . . Swartz was not an MIT student, alumnus, or staff member. MIT was not a party to the case."[17]

Limited involvement went beyond just avoiding public statements or being impartial with regard to the prosecution and the defense. MIT did not form an opinion about the nature of the charges against Aaron Swartz or the merits of the case brought against him. MIT first focused in August 2012 upon what the actual charges were. (See section III.D.) Until the suicide of Aaron Swartz, the MIT administration treated the case as one of many issues it was addressing, not as an issue of central importance. Similarly, the MIT community did little to draw the administration more deeply into the case.

The OGC raised the issue of neutrality with administration and faculty personnel on several occasions, each time receiving support. Specifically, OGC advised MIT's Chancellor and raised the matter at meetings with the senior administration of MIT, with members of the Faculty Policy Committee, and with selected faculty. All indicated that they were in accord with this approach. A few members of the faculty expressed the view that Aaron Swartz had harmed MIT, and a few members asked the administration to advocate for Aaron Swartz.

Viewing the initial choice of neutrality, we note that this position was chosen despite the fact that Aaron Swartz had engaged in an activity that had inconvenienced MIT, both from the interruptions of JSTOR availability and from the efforts to limit and then end the downloading. MIT revisited the basic neutrality decision several times over the course of the prosecution, each time considering being more supportive of Aaron Swartz rather than maintaining neutrality, and coming to reaffirm neutrality. Part IV discusses some of the options that were available.

There were several reasons communicated to the Review Panel for maintaining neutrality, beyond the basic fact that Aaron Swartz was not formally affiliated with MIT. Here are some of the reasons the Review Panel heard during our interviews with members of the OGC and the administration:

[17] Transmittal from MIT's General Counsel.

- Aaron Swartz had used MIT's premises and network to allegedly commit crimes, he had adversely affected MIT's relationship with JSTOR, and he had seriously inconvenienced MIT's Libraries, MIT researchers, and students seeking to use JSTOR, and MIT's IS&T personnel who repeatedly tried to stop his misuse of MIT's network. MIT felt no sense of obligation toward someone who had abused the open access privileges it had provided for the convenience of guests, even if that abuse was carried out in the name of open access.

- There seemed to be little interest in the case from students or faculty or the larger MIT community.[18]

- Unlike JSTOR, which wanted the return of the downloaded articles, MIT was not seeking anything from Aaron Swartz. MIT never filed a civil suit against him for any damages, or sought restitution for the result of his actions using the MIT network.

- The criminal prosecution was a legal dispute between the United States and Aaron Swartz. Swartz had extremely competent defense counsel, and "MIT should not take any action unless Swartz's defense counsel asked us to do so . . . . We did not presume to know what would benefit Swartz's defense."[19]

- MIT faculty members had previously admonished the MIT administration for a statement it had issued on a previous criminal matter (that of Star Simpson), and some faculty members had urged the administration not to make "public statements that characterize . . . the behavior and motives of members of the MIT community whose actions are the subject . . . of pending criminal investigation."[20]

- While individual members of the MIT community are encouraged to express their opinions on controversial topics, MIT itself as an institution only rarely takes a position in a lawsuit to which it is not a party. "For MIT to express a single opinion on behalf of the entire institution, the subject must have significant bearing on MIT's institutional interests, have been subject to discussion and debate within the MIT community over time, and have inspired the personal engagement of MIT's senior leadership . . . . *U.S. v. Swartz* did not fit that description."[21]

---

[18] In all, there were only a few approaches by faculty to OGC or the administration, as described in section III.C.5, and no approaches by students.

[19] Transmittal from MIT's General Counsel.

[20] This refers to one of the resolutions advanced during the Star Simpson matter. It had failed on a close vote. See Appendix 9.

[21] Transmittal from MIT's General Counsel.

- The OGC considered how its position might affect future interactions with the U.S. Attorney's Office concerning the prosecution of students and others in the MIT community.

- Although the indictment asserted that Aaron Swartz intended to distribute the downloaded articles globally, doing so though the Internet, this was not a view shared by everyone. OGC commented that it did not know—and still does not know—what Aaron Swartz might have been planning to do with the articles, and this lack of knowledge was another reason why it believed the posture of neutrality was correct.

On June 6, 2011, MIT retained outside counsel with criminal law experience to advise and assist it in dealing with the USAO and Swartz's attorneys. By this time, MIT's neutrality policy had been established and was not significantly affected by outside counsel. But there was an additional factor concerning preserving neutrality where outside counsel did play a role: MIT's outside counsel had conversations with the lead prosecutor on August 9, 2012, and with Swartz's defense counsel, William Kettlewell, on August 10, 2012. Both conversations confirmed the view held by OGC (since at least June 2011) that MIT's opinions were unlikely to have an effect on the prosecution. The August 9 conversation (discussed in detail below, in section III.C.3) confirmed OGC's concern that a public statement might backfire, and could do harm to Swartz compared with saying nothing publicly.

In summary, MIT adopted its neutrality position soon after the arrest and maintained it basically unchanged until the fall of 2012, when the defense filed motions seeking to suppress evidence, claiming illegal actions by MIT. MIT decided that it would not be fully neutral with regard to defending anticipated possible attacks on MIT's employees or the Institute's integrity. Despite differences in alignment of the defense's interests with MIT's interests, MIT continued some aspects of its neutrality toward prosecution and defense.

III.A.4 MIT discusses possible public statements with JSTOR (June 2011)

In the months after the arrest, MIT and JSTOR continued their discussions about the events that had led to the arrest. MIT's side of this conversation was communicated mostly through the MIT Libraries. On January 31, 2011, JSTOR asked MIT whether "[W]e can have a conversation about the situation . . . [which] has taken on increasing importance." The reply from the Libraries was, "[L]aw enforcement has taken over the situation . . . I am strictly enjoined from discussing it with anyone other than counsel."

Over the next months, JSTOR engaged in negotiating a civil settlement with Aaron Swartz for the return of the materials, which culminated in a settlement on June 3, 2011

(as described in section II.C). MIT was not involved in these discussions. On June 8, 2011, OGC informed the Libraries that MIT's outside counsel had just been contacted by Aaron Swartz's attorney (this was William Kettlewell), who told the counsel that Swartz had reached an agreement with JSTOR and asked whether MIT "was looking for anything" from Swartz (e.g., restitution). OGC said that MIT was not seeking anything from Aaron Swartz and that its view was that MIT should not take a position on the prosecution and should generally not comment to Swartz's attorney or to the press.

Also on June 8, 2011, JSTOR notified the MIT Libraries that "the suspect in the case has surrendered the stolen records to the authorities." JSTOR felt that it had an obligation to send a letter to the publishers who provided content, to reassure them that the records had been returned with no apparent harm. JSTOR's message to the Libraries included a draft letter, which did not name MIT and which it was sending along for MIT's comment.

The Libraries reviewed the draft with OGC and the MIT News Office. MIT suggested two changes to the letter: (1) that the statement should clarify that the responsible individual was not affiliated with the university where the incident occurred,[22] and (2) to eliminate a statement that it was the school that identified the suspect (in fact it was law enforcement). JSTOR's final letter was released on June 10. The letter read in part:[23]

> I am writing to make you aware that JSTOR experienced a significant misuse of its database in which a substantial portion of the content was downloaded in an unauthorized fashion using the network at one of our participating universities. The situation has been remedied and the data are secure, though I wanted to alert you given the scale of the incident and to share additional steps we are taking to prevent these occurrences in the future.
>
> The content that was taken was systematically downloaded using an approach designed to avoid detection by our monitoring systems. Fortunately, we were able to uncover the activity and worked with the institution to isolate the source on campus and to stop it. An individual believed to be responsible for this activity was later identified. We understand this person was not affiliated with the school.

While preparing this letter, JSTOR was also exploring possible "scenarios" for issuing a statement in the event Aaron Swartz was indicted. One scenario was to issue a statement to academic libraries jointly with MIT, issued the day of the indictment. On June 15, 2011, JSTOR sent a proposed draft to MIT clarifying in its transmittal email, that "we are

---

[22] As an OGC attorney commented to the Libraries, "If and when it comes out that this occurred at MIT, I don't want people to think that this was an MIT community member."

[23] The complete letter is included in Appendix 12.

currently NOT planning to send out a message such as this, we are trying to prepare in case we need to move quickly in various circumstances, and I want to be in close communication with you to be prepared." The proposed draft gave a summary description of the downloading, and it concluded:

> Finally, we believe it is important to emphasize that we have no specific interest in the criminal case announced today. We have taken the steps we believed necessary to resolve the incident. The current investigation is led by the United States Department of Justice, and while we are cooperating in response to the subpoenas we have received, we cannot comment on it.

MIT expressed concerns about the text of the letter and whether such a letter was advisable at all. The Libraries told JSTOR that "they [OGC and the MIT News Office] believe in general that the less MIT says, the better. We can't really discuss the details of the ongoing criminal investigation and possible indictment, nor do we want to interfere with the processes and duties of the USAO," and "in my opinion neither JSTOR nor MIT should under any circumstances comment publicly on the details of the incident until the criminal justice system had completed its work and a formal determination of the facts had been made."[24]

This statement was never issued, nor was it further discussed with MIT, but JSTOR did issue a press release on July 19, the day that the indictment naming Swartz was unsealed.[25] (See section II.C.) MIT was not notified of that statement in advance, and did not issue a statement of its own.[26]

III.B Events around the Time of the Indictment (April 2011–September 2011)

At about the time of the JSTOR settlement, the Swartz defense team began to realize that getting JSTOR to settle would not be sufficient to "call off" or soften the prosecution. Early in June, William Kettlewell made attempts to talk to MIT through its newly retained outside counsel, wanting to know MIT's position. On June 7, Kettlewell sent an email to the outside counsel asking, "What's up on your front?" Outside counsel informed OGC of this inquiry, and OGC responded by email explaining that "MIT cooperates with law enforcement and it will do so as it concerns Mr. Swartz. However, MIT is not taking a position concerning whether he should be prosecuted."[27]

---

[24] Email from MIT Libraries to JSTOR, June 15, 2011, and June 16, 2011, respectively.

[25] <http://about.jstor.org/news/jstor-statement-misuse-incident-and-criminal-case>

[26] JSTOR told the Review Panel that one reason it did not give MIT advance notice of its July 19 statement was its inference drawn from the June communications that MIT did not want to be involved.

[27] OGC informed the MIT Libraries about the conversation, as noted in section III.A.4. The OGC email to Kettlewell was the first time that MIT had publicly expressed that it would not take a position on the indictment.

III.B.1 Early overtures to MIT in support of Aaron Swartz (April 2011–June 2011)

Prior to mid-2011, the Aaron Swartz defense team focused its attention on persuading JSTOR to lobby the USAO to forgo a prosecution, beginning with negotiating with JSTOR for return of the downloaded documents. (See section II.C.) MIT had no involvement in this activity. As early as June 6, 2011, William Kettlewell had spoken with MIT's outside counsel, telling him that Swartz had reached an agreement with JSTOR and asking whether MIT "was looking for anything" from Swartz. This was taken by MIT as Kettlewell wanting to report back to the prosecutors that the "victims" named in the indictment were not seeking anything from Swartz and were generally satisfied with his efforts to make amends.

During these same weeks, Aaron Swartz's father, Robert Swartz, undertook to directly interact with the Institute, independently from his son's lawyers. Robert Swartz had done his undergraduate work at MIT, and attended MIT both as a graduate student and a special student. He had been a consultant at the MIT Media Lab since 2000. He expressed frustration that the "human side of the story" was not getting through to MIT, and felt that he would be more productive at getting help for his son by appealing directly to MIT leaders rather than working through attorneys.

On June 13, Robert Swartz wrote to the incoming Director of the Media Lab ("the Director") explaining that his son had been arrested by the MIT Police in January and was now under the threat of a federal indictment. "I wondered if we could speak about how we could enter into a dialog with MIT to help resolve this," he asked. The Director was new to MIT and to the United States, and thus his own contacts within MIT and his knowledge of the American criminal justice system were limited. Nevertheless, he made several efforts on Robert Swartz's behalf to engage the Institute.

Over the next week, the Director sent emails to several people at MIT. One, sent to OGC on June 21, included:

> I'm not sure if you're aware of this incident, but last year and into this year, there was an incident where a computer was put into the basement of one of the MIT buildings and was used to download the database of JSTOR. This was investigated by the MIT Police and a young man named Aaron Swartz was arrested in January. He is now on trial for a Federal felony for unauthorized access to a computer system. This is a prison sentence I gather. . . .
>
> The family have settled with JSTOR and returned all of the stolen materials and JSTOR has decided not to press charges. . . .

> Aaron's brother Noah is a student in the Media Lab and his father works for me in the IP department. Aaron himself works at Harvard. I wonder if there is any way that MIT might consider this a "family matter" and consider helping to try to limit the extent of the punishment and at least prevent Aaron from going to prison on a felony charge. Obviously it was a stupid thing to do, but the weight of the possible sentence seems quite harsh in my personal opinion.
>
> Apparently a grand jury is meeting to render an indictment on Wednesday and there is really only one more day to provide any input into the process. Since it is a criminal case and the prosecutor needs to prove beyond reasonable doubt that it was unauthorized, I think MIT is in the position to "cast doubt" if it desires.

OGC sent a short response to the Director that it was generally aware of the situation with Aaron Swartz, and in a follow-up phone conversation explained that MIT was not pursuing criminal charges, was not making a claim, and had nothing to settle with Swartz; and that MIT would possibly handle the matter differently if Swartz had been an MIT student. No action resulted from these communications.[28]

Among Robert Swartz's approaches was to try to get his son an appointment at MIT, so as to formally bring him in as part of the MIT community. However, the Director could not find a legitimate reason to bring him into the Media Lab, and that approach did not succeed in generating an appointment. Another approach was to have MIT "settle" with Swartz, similarly to how JSTOR had settled: if MIT thereafter would say that it suffered no harm, then the prosecution's case might be undermined. This approach did not generate a settlement agreement (see section III.B.4).

III.B.2 The indictment: Unauthorized access

The indictment against Aaron Swartz was returned on July 14, 2011, and unsealed on July 19. The lead prosecutor sent a copy to MIT's OGC on July 19. Section II.B.2 (footnote 29) lists the charges in detail. MIT was not given advance notice of the indictment or the charges, nor was MIT involved in formulating the charges. As discussed in the next section, MIT was expressly named as one of two victims of Aaron Swartz's conduct, the other victim being JSTOR. Among the charges was that Aaron Swartz had violated Section 18 of the United States Code §1030 (the Computer Fraud and Abuse Act, or CFAA) by "accessing the MIT network without authorization" or by

---

[28] OGC told the Review Panel that it had attached no particular significance to the Director's use of the phrase "unauthorized access" or considered that this might be referring to the Computer Fraud and Abuse Act. Nor did it consider that MIT might, in the Director's words, be in a position to cast doubt on the charges.

"exceeding authorized access"; and that the damages to MIT and JSTOR exceeded $5,000. For the CFAA, authorization of access to the MIT network is based on the rules of access set down by MIT (just as authorization of access to JSTOR documents is based on the rules set down by JSTOR). Thus MIT might be expected to play an important role in the interpretation of its access rules. Should there be a trial, MIT employees would likely be witnesses called to explain the rules. Moreover, during the plea bargain process, MIT might be asked to comment on the rules and could take the opportunity to come forward with a statement about the rules.

Despite the importance to the legal proceedings of MIT's interpretation of its own rules, the initial investigation paid little attention to how these rules applied to the authorization of people attempting to access the network. According to the Cambridge Detective involved in the prosecution, he asked repeatedly whether the laptop found in the closet was authorized to be there and to do what it was doing: he was told "no." On the other hand, the Review Panel spoke with personnel from IS&T and OGC, and with MIT's outside counsel, about their interviews and discussions with federal law enforcement during the entire period of the government's prosecution, from the date of Swartz's arrest until his suicide. They reported uniformly that no one from the government's investigatory team asked specifically whether Swartz—the person, as opposed to his laptop—was allowed to use MIT's network, nor were they specifically asked whether this use constituted access without authorization or access that exceeded authorization. (This distinction between the *person* and the *laptop* and its significance for the CFAA is discussed in Appendix 11.) Similarly, until very late 2012, Aaron Swartz's defense team did not raise any questions about this issue in their interviews with MIT personnel or their discussions with OGC or with MIT's outside counsel. Nor did Swartz's defense raise this issue with MIT prior to filing its motions to suppress (see section II.B.2), which referenced the allegations of unauthorized access and MIT's policies with regard to those allegations.

Consistent with its neutrality posture (see section III.A.3), MIT paid little attention to the details of the charges. MIT did not undertake its own analysis of whether the crime of gaining unauthorized access or exceeding authorized access of MIT's network had occurred.[29] Nor did it bring to the attention of the USAO or the defense the possibility that MIT's policies and practices cast doubt on this allegation in the indictment, as the Media Lab Director had noted that MIT could consider doing (see section III.B.1).[30]

---

[29] Advising MIT on the appropriateness of the prosecution's conduct during the criminal case was within the scope of MIT's outside counsel's function. Both OGC and outside counsel agree on this.

[30] This is in contrast to the case of *United States v. LaMacchia*, a prosecution brought in 1994 by the same USAO against an MIT student, where MIT informed the USAO during the pre-indictment investigation that David LaMacchia's use of the MIT network was not unauthorized, which led the USAO

III.B.3 MIT as "victim"

MIT was named in the indictment as a victim of Aaron Swartz's alleged crime (see Appendix 13 on legal procedure). Consistent with the naming in the indictment, the USAO notified MIT that it was a victim in 11 routine emails sent in late 2011 and throughout 2012.[31]

As a victim, MIT had standing to state a position about the prosecution and sentencing of Swartz, which was discussed within OGC and with outside counsel. MIT recognized that Aaron Swartz had harmed the Institute with his downloading. Despite that, with MIT's stance of neutrality, this concept of "MIT as victim" meant little to MIT: the Institute simply did not view itself as a victim in anything other than the most technical sense.[32] Indeed, as noted in section III.A.2, above, and section III.B.3, below, MIT had conveyed to the USAO its lack of interest in prosecution (neutrality) well before the arrival of the first victim letter in December 2011. It placed no significance on getting the routine victim notification emails; it sought nothing directly from Aaron Swartz, and it did not initiate a civil suit.

MIT, whether as a "victim" or otherwise, hoped to avoid the expenditure of time and resources that it would incur if a trial took place, and it wanted to protect its employees from having to testify and thus be exposed to cross-examinations designed to challenge their credibility for the purpose of advancing the interests of the defense. Thus, it would be advantageous to MIT if the parties achieved a resolution that would avoid trial, although MIT did not express a view on what that resolution should be. MIT explained to the lead prosecutor that it was not interested in the prosecution; conversely, MIT sought to make clear to the defense that they should not anticipate that it would lobby the prosecution on behalf of Aaron Swartz.

III.B.4 Robert Swartz meets with MIT's Chancellor (September 2011)

After the indictment, Robert Swartz continued his efforts to persuade MIT to influence the prosecution. His primary thrust was to arrange a meeting with someone in MIT's senior administration in order to achieve a JSTOR-type civil settlement with MIT that

---

to pursue other charges, but not to pursue a charge of unauthorized access. Appendix 9 provides details of the case. As LaMacchia was a student and Swartz was a "guest," analysis of the rules for access would differ between the two cases.

[31] MIT received routine Victim Notification Statements from the Department of Justice by email on the following dates: December 27, 2011, January 23, 2012, March 20, 2012, April 30, 2012, May 29, 2012, August 13, 2012, August 20, 2012, September 21, 2012, December 5, 2012, December 17, 2012, December 21, 2012. These statements notified MIT about scheduled status conferences and other court hearings.

[32] Notably, at least one senior-level person within MIT Libraries felt that Swartz's conduct had seriously interfered with the Libraries' operations.

could then be used to lobby the USAO on his son's behalf. He first asked for such a meeting on August 20, 2011.

A meeting was arranged between Robert Swartz and MIT's Chancellor for September 14, 2011. Robert Swartz met with the Chancellor, who was accompanied by an attorney from OGC.[33] During the meeting, the Chancellor told Robert Swartz that MIT was not pressing charges, that it was being neutral, that the USAO was prosecuting Aaron Swartz, and that MIT was providing information as required by the legal process.[34]

Robert Swartz wanted MIT to help his son. To that end, he proposed that MIT make a "settlement" with his son, similar to that with JSTOR, for the defense to use to try to influence the USAO. However, unlike JSTOR (which wanted the download secured), MIT did not want anything from Aaron Swartz and had no intention of filing any lawsuit against him, and saw no point in a settlement.

The meeting was extremely disappointing to Robert Swartz. It seemed to him that MIT was not only denying his request, it was denying the very basis of the help he was seeking, in a manner that seemed to afford no way forward. Given his background at MIT, this seemed to him a shocking failure of compassion. At one point in the meeting, he reportedly asked, "Why are you destroying my son?" The Chancellor replied that this was not MIT's intention or desire.

Robert Swartz also disputed the assertion that MIT was acting in a neutral manner, asserting that the defense could not get any assistance from MIT, particularly access to persons, documents, or answers to questions about the network or logs.[35] Robert Swartz

---

[33] There is some confusion and dispute regarding why MIT's Chancellor had an attorney present while Robert Swartz did not. The Chancellor wanted this particular OGC attorney present because this attorney had been actively involved in the oversight of the matter for MIT. The Chancellor informed Robert Swartz of this when arranging the meeting and suggested that he "also invite a legal representative so we are on equal footing." When the meeting was scheduled by the Chancellor's assistant, Robert Swartz responded, "I have confirmed this with Bill Kettlewell Aaron's attorney and look forward to the meeting." As the meeting approached, MIT learned that Kettlewell did not want to participate because he thought that the meeting would accomplish more if it occurred among principals rather than with attorneys present. On September 12, the OGC attorney spoke with Kettlewell and received express permission for him—an attorney—to participate in the meeting and speak directly with Robert Swartz despite Robert Swartz not being represented by counsel during the meeting. (At this time OGC was unclear whether Kettlewell represented Robert Swartz or Aaron Swartz; the rules of professional responsibility place significant restrictions on attorneys communicating with non-represented persons, or persons who are represented by counsel when such counsel are not present.)

[34] During this conversation, the OGC attorney said that MIT had not turned over anything to the government without a subpoena. In fact, this was not true, as the attorney offered during his interviews with the Review Panel. MIT had turned over material prior to subpoena, as explained in section I.B. Given the time that had elapsed, the attorney had not remembered the material produced during this period.

[35] At this point in time, Swartz's defense counsel had not requested from MIT any documents or interviews, either informally or by subpoena. Also, at this point in the prosecution, the defense did not have the ability to issue a Rule 17(c) subpoena, whereas MIT had produced, and continued to produce,

also accused MIT of breaking its own rules and breaking the law by turning over various items to the government in violation of the rights of his son.

The meeting did not change MIT's policies with regard to the Swartz prosecution. Shortly thereafter, due to a life-threatening illness experienced by his wife (Aaron's mother), Robert Swartz was forced to curtail some of his lobbying efforts on behalf of his son.

III.C MIT's Contacts with Prosecution and Defense (October 2011–September 2012)

Little happened from MIT's perspective in the months following September 2011. There were few communications between the prosecution and MIT after the indictment, except for occasional emails from the government seeking bits and pieces of information relevant to the government's case.[36] MIT's outside counsel had no communications at all with the USAO throughout 2011. With the exception of five routine victim status notifications sent between December 27, 2011, and May 29, 2012, there were no prosecution communications with OGC or its outside counsel after Oct. 5, 2011, until they resumed with a phone call on August 9, 2012 (see section III.C.3).

Contact with the defense was also limited. William Kettlewell made several phone calls to MIT's outside counsel during September 2011, both before and after MIT's meeting with Robert Swartz in September 2011.[37] Kettlewell also forwarded to MIT's outside counsel a copy of the JSTOR agreement that Aaron Swartz had signed. Andrew Good withdrew as Aaron Swartz's attorney in late October and was replaced by Martin Weinberg. Robert Swartz was dealing with his wife's illness. For all practical purposes, communications between Swartz's defense team and MIT remained dormant until the spring of 2012.

III.C.1 Responses to defense inquiries are slow (May 2012–August 2012)

In late April 2012 and then again in May, William Kettlewell and Martin Weinberg met with MIT's outside counsel seeking to enlist MIT's support in lobbying the USAO to

---

documents and information to the government pursuant to the pre-indictment grand jury subpoenas with which it had been served. See Appendix 10.

According to an email that William Kettlewell sent to Robert Swartz before the meeting, OGC had told Kettlewell that MIT "would feel bound to inform [the lead prosecutor] that they were meeting with us as well as what transpired at the meeting." When questioned about Kettlewell's email, OGC explained that it did not in fact discuss the substance of this meeting with the prosecution.

[36] This information was provided by MIT under what it believed to be the umbrella of the two previously served grand jury subpoenas. MIT's outside counsel was not involved in these communications.

[37] Some of these concerned a draft protective order then being considered by the USAO and the defense to protect the confidentially of MIT's documents and the privacy of its employees during the discovery phase of the prosecution.

drop its demand for jail time. They also suggested that the packet stream capture (see section I.B, item 4) might have been a privacy violation. They asked that MIT make a decision to take a position favorable to the defense with the USAO concerning the prosecution, and they asked for a meeting with MIT to discuss this.

The defense attorneys did not get a timely response to these requests. Kettlewell called and spoke with MIT's outside counsel five times during May seeking a meeting with MIT; in each of June and July, he called twice; in August, he called four times; and in September he called once more, before finally obtaining a confirmatory email for such a meeting from MIT's outside counsel. Robert Swartz and defense counsel for Aaron Swartz were uniform in their complaints to the Review Panel that MIT failed to respond in a timely manner, although varying in where they placed the blame among MIT's OGC, its administration, and/or its outside counsel.

For its part, MIT points to a variety of reasons why its responses were slow, without denying that they were, in fact, slow. Some explanations are mundane: during the period in question, activities such as commencement, corporation board meetings, and vacations for senior officials took place. Also, there is some uncertainty as to how many of Kettlewell's individual telephone calls to MIT's outside counsel were passed on to the OGC, although the thrust of Kettlewell's continuing desire for a response was definitely transmitted. OGC knew that it needed to get back to the defense in spring and mid-summer 2012, but it wanted to get some information first on the status of the case. Most important, OGC's attorneys felt that they did not know what Swartz's defense team wanted. From their perspective, MIT had already made clear that the Institute would remain neutral. They did not realize that the defense team was seeking a meeting about a specific proposal, as opposed to continuing general discussions regarding Aaron Swartz (perhaps in the hope that MIT's position might change).

Martin Weinberg has provided for the Review Panel, in writing, his description of what the defense team sought from MIT:

> For over 6 months Bill Kettlewell and myself had engaged in a joint effort which Bill had begun in June of 2011 through telephone conversations with [an attorney in OGC] and a meeting between Bob Swartz, [the Chancellor], and [the OGC attorney]. The joint initiative that I participated in with Bill began in April of 2012 and included meetings and telephone conversations with [MIT's outside counsel] followed by a meeting with [MIT's outside counsel], the Chancellor, and [MIT's General Counsel]. The single focus of our initiative was to actively seek MITs affirmative assistance in supporting a plea initiative with the USAO that would resolve Aaron's federal case without a trial (and without evidentiary hearings on contested pretrial issues involving the warrantless

> interceptions of electronic communications) and which would spare Aaron the risk of a prison sentence.

III.C.2 Robert Swartz writes to MIT's President

Towards the end of July 2012, Robert Swartz again contacted the Media Lab Director, asking him to help arrange a meeting with MIT's senior administration. The Director asked Swartz to draft a letter, which he then forwarded to MIT's President,[38] Chancellor, and General Counsel. The Director forwarded the letter on August 10 under the following cover:

> I'm not sure if you've been tracking Aaron's case, but this is an email from his father who works for us part-time at the Media Lab as an IP consultant. Would someone at MIT be willing to meet with him? I think you've met with him once in the past near the beginning of this process.

Robert Swartz's letter follows:

> As you know my son Aaron is under federal indictment for alleged acts that occurred at MIT. Although he settled with JSTOR the aggrieved party, and they indicated that they did not want the prosecution to go forward the case has not been resolved. We think there are both legal and non-legal issues that you are not aware of and urgently ask for a meeting with [MIT's Executive Vice President] and [MIT's President].
>
> It is the non-legal issues in the context of the MIT community and a possible trial that most urgently need to be considered in the meeting. The urgency of the meeting is due to fact that the prosecutor has given us a deadline of Wednesday to resolve the case or go to trial and we have a meeting Monday with the head of the criminal division that requires hard decisions.
>
> I am willing to meet at any time even over the weekend. Please let me know the earliest time that we can meet.
>
> Thanks in advance for all of your help.

The President forwarded this letter to the Provost, the Chancellor, and the General Counsel with a note saying that that they should contact him (the President) if necessary.

On August 12, 2012, the Director informed Robert Swartz that he had heard from the Chancellor and "they are now reaching out to you." This eventually resulted in Swartz's

---

[38] MIT's current President assumed office in July 2012. Prior to that, he was MIT's Provost.

(second) meeting with the Chancellor on September 12, described below (see section III.C.4).

III.C.3 MIT's outside counsel speaks with the lead prosecutor (August 9, 2012)

OGC knew that it needed to get back to the defense in spring and mid-summer 2012, but it wanted to get some information first on the status of the case. It also wanted to "deliver a message" to the USAO that it was not advocating a jail sentence. OGC asked its outside counsel to speak with the USAO.

On August 9, 2012, MIT's outside counsel had a 45-minute telephone conversation with the lead prosecutor. They covered the following points:[39]

- The prosecutor praised MIT's conduct before and after Aaron Swartz's arrest. He described MIT's approach in tracking down Swartz and intercepting his communications as "reasoned" and "nowhere near cowboy conduct," and said that he had "the deepest of respect for their approach to the case."

- The prosecutor expected Weinberg to file motions challenging the government's and MIT's collection of electronic evidence. He expected that hearings would be held, and numerous MIT witnesses, some six to 10, would have to testify.

- The prosecutor said that the government had been extremely reasonable in this case, and has made its best offer. The government believed that jail time was appropriate. If this case had involved solely hacking into MIT's system, the government might feel differently, but the case also involves the unauthorized downloading of intellectual property that cost millions of dollars to create.

- The government was willing to agree to a "very strong downward departure" from the sentencing guidelines, but there were some lines below which the USAO would not go.

- MIT's counsel noted that no one at the Institute was looking forward to the time, disruption and stress involved in testifying at hearings and trial. The prosecutor's response was that it disturbed him whenever a defendant "systematically re-victimized" the victim, and that was what Swartz was doing by dragging MIT through hearings and a trial. He analogized attacking MIT's conduct in the case to attacking a rape victim based on sleeping with other men.

---

[39] This material is taken from a memorandum provided by MIT's outside counsel to OGC, dated August 10, 2012. Where phrases appear in quotes in this material, the same phrases appear, also in quotes, in the memorandum.

- MIT's counsel stated that, while the government might believe that jail time was appropriate in this case, the government should not be under the impression that MIT wanted a jail sentence for Aaron Swartz. The prosecutor responded that the government believed that some custody was appropriate. He said the government had to consider not only the views of the immediate victims, but also general deterrence of others.

- MIT's counsel mentioned that MIT viewed itself as an educational institution, and that consistent with its overall mission it did not focus on punishment or retribution, but rather education.

- MIT did not want to act as an intermediary between the parties.

- The prosecutor said that, pre-indictment, he had wanted to approach the case on a human level, not punitively. To this extent he made an extremely reasonable proposal, and was "dumb-founded" by Swartz's response.

- The prosecutor said that the straw that broke the camel's back was that when he indicted the case, and allowed Swartz to come to the courthouse as opposed to being arrested, Swartz used the time to post a "wild Internet campaign" in an effort to drum up support. This was a "foolish" move that moved the case "from a human one-on-one level to an institutional level." The lead prosecutor said that on the institutional level cases are harder to manage both internally and externally.[40]

This conversation supported the following conclusions, consistent with OGC's earlier views:

> First, the lead prosecutor and the USAO did not care what MIT thought or said about the case, and its ability to influence a resolution was slim to none.
>
> Second, the lead prosecutor's comment about a "wild Internet campaign" orchestrated by Swartz to drum up support made MIT concerned that any public statements that MIT might make on Swartz's behalf could backfire.
>
> Third, it might be in Aaron Swartz's interests to accept the government's offer, now, before it became worse, and OGC should make it clear to Swartz's attorneys that MIT was remaining neutral, i.e., that it would not advocate in his favor, so as

---

[40] The only Internet campaign occurring during this period that has been identified by the Review Panel is the statement and petition drive conducted by Demand Progress, referenced in section II.B.2. As noted there, the statement was co-drafted by the Director of Demand Progress and Quinn Norton. We do not know what the lead prosecutor meant by "institutionalizing" a prosecution, and we do not comment on the implications of doing so based upon a public lobbying effort undertaken by or on behalf of a criminal defendant.

to not mislead the defense into delay that might result in a less favorable plea offer being available at a later date.

III.C.4 Robert Swartz meets again with MIT (September 2012)

On September 12, 2012, Robert Swartz had another meeting at MIT with MIT's Chancellor and its General Counsel. Robert Swartz made four points:

> First, he wanted MIT to make a public statement. This, the Chancellor and General Counsel explained, MIT would not do, although they did not explain about the outside counsel's August 9 meeting with the lead prosecutor (see section III.C.3) or the conclusions MIT drew from it.[41]
>
> Second, Robert Swartz connected the matter of his son to that of Star Simpson,[42] arguing that the Star Simpson matter was a precedent that would allow MIT to make a statement. The Chancellor and the General Counsel took a different view, explaining that after MIT had made those statements its administration had been (justly) reprimanded.
>
> Third, he argued that MIT was assisting the government more than it was assisting his son. The General Counsel reiterated that MIT's policy was "neutrality." Mr. Swartz disputed whether that was in fact the case, citing, among other examples, that MIT had turned material over to the Secret Service without subpoena.[43]
>
> Fourth, Robert Swartz claimed that, in the past, MIT's policy had been to turn off troublesome email connections rather than to call in the police. The General Counsel explained that MIT had tried to terminate Aaron's access to MIT's network several times, but he had managed to evade these attempts.

Robert Swartz also accused MIT of violating wiretap laws and its internal policies in its collection of electronic communications of his son and providing them to the prosecution, and of violating his son's privacy rights in doing so.

---

[41] As a general matter, for a third party to convey information from one party to a lawsuit to the opposing party without permission would be very likely to cut off the flow of information if that conveyance of information were to be perceived.

[42] See Appendix 9 for a discussion of the Star Simpson matter.

[43] MIT did turn over material without subpoena in the first few days after the arrest. (See section I.B and Appendix 7.) Appendix 10 gives the Review Panel's perspective on the legality of MIT's provision of this information. After January 27, 2011, there was no document provision to the prosecution without a subpoena. But even had the material been turned over pursuant to subpoena, it is likely there would have been disagreement about whether MIT had acted "neutrally." As noted in section III.A.3, OGC interpreted neutrality of legal process in terms of similar responses to similar requests, rather than similar outcomes.

Overall, the meeting produced the same result as the September 2011 meeting (see section III.B.4).

III.C.5 Other contacts on behalf of Aaron Swartz

As discussed above (and below), Aaron Swartz's father and defense team approached MIT several times to ask that MIT move away from its neutrality stance and advocate for Aaron Swartz. As discussed in section III.B.1, the MIT Media Lab incoming director did so on June 21, 2011, as part of supporting a request that MIT meet with Robert Swartz: "I wonder if there is any way that MIT might consider this a 'family matter' and consider helping to try to limit the extent of the punishment and at least prevent Aaron from going to prison on a felony charge. Obviously it was a stupid thing to do, but the weight of the possible sentence seems quite harsh in my personal opinion."

Otherwise, there were very few direct contacts made with the MIT administration to encourage a change on the part of MIT from neutrality to advocacy. MIT's student newspaper*, The Tech*, reported regularly on the progress of the case, but this did not prompt any editorials or opinion pieces before Aaron Swartz's suicide. Nor did people who later criticized MIT for not advocating for Aaron Swartz approach the MIT administration making the case for MIT to advocate for him before the suicide.

The Review Panel is aware of only three further contacts requesting advocacy for Aaron Swartz. One senior faculty member, who had worked with Aaron Swartz, tried to solicit MIT's support on Swartz's behalf. From the last week in August through mid-September, 2012, he met (separately) with MIT's Chancellor, Provost, General Counsel, and another OGC attorney. He advocated for active MIT support for Aaron Swartz, raising several possible options, including making a public statement of the kind JSTOR had made.[44] He told the Review Panel that he had sought support because he believed that an incredible miscarriage of justice was in the works; that while Aaron Swartz was a tireless fighter for right, he was also vulnerable; that a felony could affect Aaron Swartz's career; that he liked and respected Aaron Swartz in many ways; and that the law was being seriously abused. He told the Review Panel that Aaron Swartz's action was the sort of thing that historically would have prompted a certain pride, not criticism, at MIT.

---

[44] There are differing recollections as to whether any of the discussions included phoning the prosecutor in support of Aaron Swartz. According to the recollection of the faculty member, his meeting with OGC included the suggestion that MIT phone the prosecutor to say that MIT would prefer them to drop the charge, or that MIT did not have any issue with Aaron. OGC reports that the overwhelming focus of this meeting was on a public statement and does not recall any mention of a private statement. The faculty member later told the Review Panel that he left these meetings with the impression that MIT would not make a public statement, but that OGC would phone the prosecutor.

The meetings with this faculty member did not result in a movement to advocacy. MIT's responses included multiple reasons for supporting neutrality (see section III.A.3 for a full list of reasons the Review Panel heard). OGC and other senior MIT administrators said that they felt MIT should not take any action on Aaron Swartz's behalf unless Swartz's defense counsel asked it to do so. Members of the administration and OGC with whom this faculty member spoke did not tell him about the recent conversation between MIT's outside counsel and the lead prosecutor. The outcome of that conversation supported OGC's belief that making any statement to the USAO would likely not help, and making a public statement could actually harm, Aaron Swartz's defense.[45]

In October 2012, a faculty member who was active in MIT's Open Access activities spoke with Robert Swartz and later contacted the Director of Libraries, an OGC attorney and the Chancellor, asking if MIT could do more for Aaron Swartz. He told the Review Panel that his main contention was just that the response of the prosecutor was utterly disproportionate, and MIT should do whatever it could.[46]

While the faculty members were reminded that they were free to make public statements or private statements to the prosecutors, they did not do so.

Considerably earlier, on November 13, 2011, a leader in the global movement for open access to scientific publications (not affiliated with MIT) emailed MIT's then President on behalf of Aaron Swartz, whom he had known well for some time. He wrote:

> I know that the case is in the hands of the public prosecutors, that MIT is not in the position—even if it wanted to—to halt the fearful procedure. . . . For a person [like Aaron Swartz], time in prison would surely be fateful, unbearable, in the worst case, deadly.
>
> I do not know the American legal system well enough, but I think that the stand of your University—which has done so much with its Open Courseware for advancing access to the finest academic works—would have an impact on the outcome of the legal process. A term in prison

---

[45] The private statement MIT had made to the lead prosecutor was similar to JSTOR's pubic statement. JSTOR wrote: "Once this [returning the documents] was achieved, we had no interest in this becoming an ongoing legal matter." (See <http://about.jstor.org/news/jstor-statement-misuse-incident-and-criminal-case>.) MIT's outside counsel did inform the lead prosecutor that MIT, as an educational institution, did not focus on punishment for Aaron Swartz, and that the government should not be under the impression that MIT wanted a jail sentence for him. (See section III.C.3.) But note that JSTOR's private statement to the USAO was stronger (and not neutral). Not only was JSTOR not pressing for prosecution: it preferred that no charges be brought. (See section II.C.)

[46] Another approach to the administration was by the lead author of this report, who phoned an OGC attorney in April 2011 to ask if OGC was handling the case, without advocating any particular action for MIT. Robert Swartz also spoke with this report's lead author in August 2012, and told him of the defense's contention that MIT had violated the Stored Communications Act as later alleged by Martin Weinberg (see section III.D.2), and the report's lead author advised OGC of this.

> would not only deeply and perhaps irrecoverably harm Aaron Swartz, but would be irrational, compared to the possible public benefit of community work that Aaron Swartz would be capable of doing by using his unique and brilliant technical skills and surprising knowledge.
>
> In the hope of your understanding and with thanks for having read my letter,"[47]

The President referred the email to the Chancellor, who consulted OGC and wrote back: "Thank you for expressing your concern about Aaron's future, and sharing your perspective, which we will certainly take into account." In response was written: "Thank you for your frank response. Despite the complexities of the situation, allow me to hope that your University will try to make use [of] all available means and fora not to ruin the life of this extremely talented, vulnerable, naive, and incautious, unique young man."

III.D Events in Anticipation of Trial (August 2012–October 2012)

Toward the end of August 2012, the USAO began asking for MIT employees to be made available for witness interviews and preparation. MIT's General Counsel informed the senior administration at the end of August that there would likely be a trial and reminded them of MIT's neutrality position. At the President's request, the General Counsel consulted with selected faculty members, including the Chair of the Faculty, about whether a discussion of the Swartz matter at MIT's Faculty Policy Council might be appropriate. The Faculty Chair consulted with the Associate Chair and the Secretary of the Faculty, and they told the General Counsel that such a discussion would not be necessary, and that there was general support for MIT's neutrality posture.

With talk of witness preparation, it became clear that the Swartz matter was probably not going to be resolved without a trial, and that it would require a significant amount of time from some MIT personnel. This prompted OGC to make an inquiry into the government's theory of the criminal prosecution. In late August 2012, OGC asked MIT's outside counsel to brief them on laws alleged to have been violated and the facts pertaining specifically to MIT upon which the criminal aspect of the Swartz's conduct might turn, and outside counsel conducted what he characterized as a "thumbnail analysis" of the indictment.

Discussions among MIT lawyers included recognizing that the government had the burden of proof in the prosecution, and therefore would want to interview more personnel

---

[47] The letter also reported that Aaron Swartz had attended a meeting that included a discussion of how much it would cost to get JSTOR to open up its archive for the public and how that exceeded the funds available to the group at the meeting. He wrote: "My fear is that our conversation at that meeting played a role in Aaron Swartz's unfortunate decision."

than would the defense; nonetheless, OGC's view here was that MIT should give the defense some of the same assistance as was given to the government (making witnesses available and recommending personnel who could educate the defense attorneys as to MIT's networks and its Library policies and practices). The guiding policy was to accommodate "reasonable requests" by the defense, taking into account such things as where the interviews would take place and how long they would take.

In mid-September, the lead prosecutor asked to interview 11 MIT employees, who were made available. Both MIT's outside counsel and an OGC attorney were present for the interviews.

On September 12, 2012, the USAO obtained a superseding indictment (described in section II.B.2). MIT's OGC perceived this as an escalation by the USAO in the prosecution. It served to reinforce the view, already well developed as a result of the August 9 conversation between MIT's outside counsel and the lead prosecutor (see section III.C.3), that MIT had no influence over the USAO in the matter.

III.D.1 The defense asks MIT to oppose jail time (September 2012–October 2012)

Aaron Swartz's defense team met with MIT on September 28, 2012. Present on behalf of Swartz were Martin Weinberg and William Kettlewell. MIT's representatives were MIT's Chancellor, its General Counsel, and its outside counsel. Weinberg asked if MIT representatives would accompany the defense to a meeting with the federal prosecutors and support their plea for no jail time as a condition of any guilty plea by Swartz. MIT's representatives responded that they would consider this.

After this meeting, OGC and MIT's outside counsel had several concerns about the defense's request that they join a meeting with the federal prosecutors. They discussed who should go, and whether any faculty should be among those attending, if such a meeting occurred. There was serious concern that, given MITs neutrality position, whatever MIT was prepared to contribute would be of no value to Aaron Swartz. And there was skepticism about whether the lead prosecutor would be interested in hearing MIT's position: he had already made it clear that he would not be influenced by it. Weinberg told the Review Panel that he in fact agreed with this assessment of the lead prosecutor's stance. But his plan was not to hold the meeting with just the lead prosecutor or with other higher-ranking Assistant U.S. Attorneys, but instead to meet with the U.S. Attorney herself.[48]

[48] Weinberg told the Review Panel that he informed MIT of this plan, but neither the two OGC attorneys who were involved, nor the Chancellor, recall him explaining this.

Ultimately, MIT decided that it would be willing to participate in such a meeting. The decision was made that the Chancellor and the General Counsel would attend the meeting, and no other faculty would accompany them. It was decided that MIT would maintain the position of neutrality at such a meeting.

MIT's outside counsel informed Weinberg that MIT representatives would be willing to attend a meeting at the USAO if he (Weinberg) arranged it, and that MIT would make the following points:[49]

1. MIT is not seeking any particular outcome, such as Aaron Swartz's conviction or, if convicted, that he receive any particular sentence.

2. Members of the MIT community knew and admired Aaron Swartz and would consider it a great loss if he were deprived of the opportunity to continue his work.

3. If asked by the USAO, the Chancellor and General Council would have to admit that some members of the MIT community held views critical of Aaron Swartz's conduct.

This was communicated to Weinberg on October 26. When it was received, the defense team felt that MIT's stance would be of no value in advocating with the U.S. Attorney and decided not to go forward with such a meeting. Elliot Peters, who had replaced Weinberg as Swartz's lead defense counsel at the end of October, informed MIT's outside counsel of this decision in early November.

III.D.2 The defense moves to suppress evidence (October 2012)

At the time of the September 28 meeting, the Swartz legal team was facing an October 5 deadline for the filing of motions to dismiss and to suppress evidence. During the meeting, Weinberg explained that he would soon have to file those motions, and they would accuse MIT of violating federal law, the constitutional rights of Aaron Swartz, and MIT's own internal policies as those policies would affect the privacy of Swartz; and they would accuse MIT of acting in concert with federal law enforcement in furtherance of these violations.

The Review Panel found that the views of those who attended this meeting differ on the nature of Weinberg's description of these motions. Some saw it as a threat that MIT would be embarrassed if the case went to trial, and so MIT should act to resolve things in Aaron Swartz's favor; others saw it as a matter-of-fact discussion of what the legal defense had to do in order to zealously represent its client, as required by the rules of

[49] Transmittal from MIT's General Counsel.

professional responsibility for attorneys.[50] Ultimately, OGC decided to ignore the possibility that Weinberg might have wanted to pressure MIT with his presentation, and instead focus on what to do about the request to meet with the U.S. Attorney's prosecutors.

On October 5, Martin Weinberg filed six motions: a motion to dismiss the indictment, and five motions to suppress evidence that the government might otherwise use at trial. These are the motions that Mr. Weinberg described in his September 28 meeting at MIT, and to which Robert Swartz had referred during his September 12 meeting at MIT (section III.C.4). Four of these motions (numbers 1, 2, 3, and 5) directly addressed conduct of MIT and its employees:[51]

> Motion to Suppress No. 1: Motion to Suppress All Fruits of Interceptions and Disclosures of Electronic Communications and Other Information by MIT Personnel in Violation of the Fourth Amendment and the Stored Communications Act[52]
>
> Motion to Suppress No. 2: Motion to Suppress All Fruits of Warrantless Searches Conducted from January 4, 2011 to January 6, 2011[53]
>
> Motion to Suppress No. 3: Motion to Suppress All Fruits of Unlawful Arrests Without Probable Cause and Search of HP USB Drive[54]
>
> Motion to Suppress No. 5: Motion to Suppress All Fruits of Searches of Acer Laptop, HP USB Drive, and Western Digital Hard Drive[55]

Taken together, these motions accused MIT and its employees of violating the Fourth Amendment rights of Aaron Swartz, the Electronic Communications Privacy Act, the Stored Communications Act, and MIT's internal policies as they applied to Swartz's expectations of privacy.[56]

---

[50] In the criminal context particularly, it is appropriate to warn a third party of what is coming, when what is coming is considered by all to be "unpleasant" but must be done to advance the cause of one's client, and where the continued cooperation of the third party is desired despite the filing or other conduct. From the perspective of a defense counsel, the purpose of this discussion was to put MIT on notice as to what was coming so as to not surprise or unnecessarily offend MIT.

[51] Motion to Suppress No. 4 concerned the Secret Service's search of Aaron Swartz's home.

[52] Doc. 59 (filed October 5, 2012), *United States v. Swartz*, Case No. 1:11-cr-10260-NMG.

[53] Doc. 60 (filed October 5, 2012), *id*.

[54] Doc. 61 (filed October 5, 2012), *id*.

[55] Doc. 63 (filed October 5, 2012), *id*.

[56] This review does not address the merits of any these motions. Appendix 10 gives the Review Panel's view of legal issues around MIT's provision of the data. And the Review Panel has not analyzed, and provides no views on, claims that Aaron Swartz's expectations of privacy were violated.

III.D.3 Effect of the suppression motions (October 2012–December 2012)

With the admissibility of the evidence against Aaron Swartz in dispute, the suppression motions had the effect of aligning MIT's interests more with the prosecution than with the defense: the government wanted to establish that MIT's conduct was entirely lawful and proper, so as to defeat the various motions to suppress. The defense wanted to show otherwise, and thus achieve the suppression of evidence that the government had obtained from or through MIT. Similarly, the government would advance the conduct, integrity, and credibility of those MIT employees who testified, while it appeared to OGC that the defense would do the opposite, attacking MIT personnel in open court. MIT decided that it would not be neutral with regard to defending MIT's employees or attacks made on the Institute's integrity.

That concern played out in the months that followed. For example, when the government's investigation had begun, in January 2011, OGC made the decision that the lead prosecutor, the Secret Service Agent, and the Cambridge Police detective could directly telephone and email previously interviewed IS&T employees without first going through an MIT attorney for follow-up questions, provided no new topics were covered (see section III.A.1). In early September 2012, after consultation with outside counsel, OGC decided to allow this direct conduct to continue during the government's preparation for the suppression hearings and trial. However, this did not occur for the defense: the defense was never given permission to interview or consult with any MIT employee without the presence of an MIT attorney, nor did it ever ask for such permission.

Another example is that MIT's outside counsel conveyed to the government what MIT wanted the government to consider in its arguments that MIT had not violated law in gathering evidence.

A third example concerns document production. When MIT provided documents in December 2012 to the defense (pursuant to subpoena), MIT's outside counsel later provided—without being asked—the same documents to the government. (This occurred in early January 2013.) However, MIT did not, reciprocally, voluntarily provide to the defense the same documents that it provided to the government. Similarly, MIT did not produce to the defense, even though requested by subpoena, documents that the defense sought from MIT but that MIT had already provided to the government. The explanation for this as offered by MIT's outside counsel is that, under the Local Rules[57] for the

[57] All federal district courts are bound by the Federal Rules of Criminal Procedure in criminal matters and by the Federal Rules of Civil procedure in civil matters. Although detailed, these rules might be considered "broad brush" rules. Each district court in the nation also adopts its own local rules, which may

United States District Court for the District of Massachusetts, a defendant is entitled to obtain from the prosecution broad categories of documents in criminal discovery.[58] Thus, MIT's outside counsel operated under the assumption that if the government obtained discovery from MIT, then the defense could get it from the government, and counsel did not want MIT to engage in duplication of effort regarding document production.

OGC's explanation for not providing these documents is similar, in that it did not want to engage in a duplication of effort, but adds that OGC was always willing to produce to the defense documents already provided to the government if, for whatever reason, the government would not produce them to the defense. As discussed above, on May 6, 2011, OGC spoke with the lead prosecutor (see section III.A.2), and during this conversation the prosecutor asked for copies, in electronic format, of the documents that had already been provided by MIT. The prosecutor explained this request by saying that he wanted these documents in such format in anticipation of providing them to the defense. For this reason, OGC operated under the assumption that whatever documents it had given to the government had been turned over to the defense.[59] As discussed below, this was apparently not the case (see section III.D.4). OGC notes that, as of January 10, 2013 (the day before Aaron Swartz took his life), MIT was in ongoing discussions with Swartz's defense counsel on this very topic.

III.D.4 Final weeks (December 2012–January 2013)

Elliot Peters replaced Martin Weinberg as counsel for Aaron Swartz at the end of October 2012. With this change, William Kettlewell's involvement in the case essentially came to an end. With the change in counsel, the focus of the defense shifted somewhat, from seeking to establish that MIT's conduct was in violation of law or policy, to placing more emphasis on the specific allegation in the superseding indictment that Swartz had accessed MIT's and JSTOR's networks without authorization. In the view of the defense, MIT's policy of open access to its network provided a weak basis for charging violations of the Computer Fraud and Abuse Act.

---

address gaps appearing in the federal rules, or may expand or reduce the applicability of specific federal rules to the extent doing so is permitted.

[58] The Applicable Local Rules of the District of Massachusetts are L.R. 116.1 and 116.2. As an example, L.R. 116.1(a)(1) provides:

In all felony cases . . . unless a defendant waives automatic discovery . . . all discoverable material and information in the possession, custody, or control of the government and the defendant, the existence of which is known, or by the exercise of due diligence may become known, to the attorneys for those parties, must be disclosed to the opposing party without formal motion practice at the times and under the automatic procedures specified in these Local Rules.

[59] Also, the negotiations surrounding the protective order concerning documents produced to the defense, which occurred in September 2011, led OGC to understand that all of the documents it produced to the government would be turned over to the defense.

This shift in emphasis was noted by MIT's outside counsel.

In December, the lead prosecutor asked to "prep" MIT witnesses for the suppression hearings. He began to inquire about MIT's trespass signs posted on its campus, and he asked ("to be followed with a subpoena") for all material pertaining to "the Swartz intrusion and data theft" prepared since MIT's last production of such information. He notified MIT's outside counsel that the suppression hearings would be held on January 25, 2013, and would include the following issues: (1) the delay on the part of the government in obtaining search warrants; (2) whether Swartz was trespassing on the MIT campus; and (3) whether Swartz had abandoned his computer on MIT property. He also indicated that he was concerned with the MIT "open campus" concept, and would issue a new subpoena for all pertinent policies and practices.

When Elliot Peters entered the case, discussions had been ongoing with MIT concerning a meeting with the USAO. He learned from MIT's outside counsel that MIT would be essentially neutral, and he did not think that this would help. Thus, he decided against having such a meeting, as had Martin Weinberg.

At this point, the focus by the defense was to deal some setbacks to the prosecution at the suppression hearing, scheduled for late January 2013. It believed that only after suffering such setbacks would the government be willing to be more lenient in its plea offers.[60] Thus, the defense plan during this period did not include trying to get MIT to support or lobby for Aaron Swartz with the USAO.

Mr. Peters says he held several discussions with MIT's outside counsel about (1) interviewing MIT personnel, to which he got no response; and (2) getting documents, to which he was told that he should get them from the government. On November 23, 2012, the defense subpoenaed MIT for production of documents. The scope of the subpoena as drafted by the defense was extremely broad: they wanted to use its scope as leverage to obtain discovery from MIT.[61]

---

[60] Mr. Peters confirms Mr. Weinberg's description of the latter plea offers made by the prosecution to Aaron Swartz: (1) he would have to plead guilty to all 13 felonies; (2) he would have to agree to four months incarceration; or (3) the government would be free to seek up to six months incarceration and the defense would be free to seek no jail time. In addition, Aaron Swartz would not be allowed to use a computer for some period of time after his conviction. This latter condition was a problem for Aaron Swartz when considering the offer. According to Mr. Peters, he advised the lead prosecutor that Aaron Swartz was "vulnerable"; that this was a reason to resolve the matter without a trial; and that he couldn't see Aaron Swartz in federal prison.

[61] As explained by Mr. Peters, he disagreed with the view that the federal rules governing the production of discovery by the government to the defense in a criminal case meant that all documents produced by a third party to the government would subsequently be turned over by the government to the defense. Rather, in his opinion, the government would turn over only some of these materials.

We noted above (see section III.D) that OGC had formed the view early in the fall that MIT should give the defense some of the same assistance as was given to the government (including making witnesses available and recommending personnel who could educate the defense attorneys as to MIT's networks and its Library policies and practices). The guiding policy was to accommodate "reasonable requests" by the defense, taking into account such things as where the interviews would take place and how long they would take. As explained by Mr. Peters, after this subpoena was served, MIT's outside counsel and the defense negotiated a more limited document production, plus the making available of two MIT employees: one from IS&T and one from MIT Libraries.

The interviews of these two MIT witnesses took place on December 11, 2012. They were conducted by one of Aaron Swartz's defense attorneys and an expert in network operations. The defense found the witnesses to be very cooperative and helpful on the issue of what comprised authorized access at MIT.[62] At the request of the defense, the identity of the expert was kept confidential from the government.[63]

MIT's initial response to the defense subpoena of November 23, 2012, was made on December 21. MIT's initial response excluded material that it had already produced to the government, due to the time-consuming and burdensome nature of document production, and MIT's expectation that the defense had or could receive from the prosecution everything that MIT had provided to them.

An email sent on January 9, 2013, from a defense attorney to MIT's outside counsel indicates that there remained open questions about the scope and adequacy of MIT's response to the subpoena. This email was forwarded to OGC. Included among the topics discussed is the defense's request that MIT provide all materials called for in the subpoena that it had previously provided to the government. OGC has explained to the Review Panel that it was willing to provide any such documents that the defense had not obtained from the prosecution.

These discussions were still under way when Robert Swartz notified MIT by email on January 11, 2013, that Aaron Swartz had taken his own life.

---

[62] Mr. Peters confirmed that the defense—similar to the prosecution—did not focus on the specific question of whether Mr. Swartz's access to the MIT network was or was not authorized. The decision to not address this question directly was a result of the defense's perception that the prosecution's theory—as to why Aaron Swartz's access to the network was unauthorized—was scattershot, ranging from Aaron Swartz's changing his computer names to his opening of locked doors. Thus, a direct answer to this question, even if favorable to the defense, would be unlikely to change the prosecution's determination to continue with the case.

[63] The witness later revealed his identity and wrote about his findings. See Alex Stamos, *The Truth about Aaron Swartz's "Crime,"* January 13, 2013, <http://unhandled.com/2013/01/12/the-truth-about-aaron-swartzs-crime/>.

Part IV: DECISION POINTS FOR MIT

Our charge in preparing this report is to "describe the options MIT had and the decisions MIT made, in order to understand and to learn from the actions MIT took."

In Parts I through III we have sought to describe MIT's actions and to place them in the context of events occurring outside of MIT. In Part V we will present some questions for the MIT community to consider, which might help with learning from this experience. This part, Part IV, responds to that portion of our charge asking us to describe options available to MIT during the investigation and prosecution of Aaron Swartz. It serves as a bridge from the facts of Parts I, II, and III to the discussion questions in Part V.

We start with the following words of caution. The act of "describing options" potentially embarks upon a sea of "might-have-beens." And considering alternatives inevitably involves hindsight: how does one maintain a perspective uncolored by the shock and tragedy of Aaron Swartz's suicide, or—knowing of him and his accomplishments—by the realization that he was the person who did the downloading and who was then arrested? We are also cognizant of a wide variety of assertions and conjectures that have appeared in public discussions of the events.

In the sections below, we identify some of the key decision points for MIT, for the purpose of understanding and learning, and of helping to frame the questions raised in Part V. Some options were available at specific times. Others were available at many times throughout the period of MIT's involvement. To provide a context for examples widely available, we have selected one or more specific times for considering such options, choosing based on the salience of the particular moment for illustrating the issues involved.

We have chosen to interpret the reference in our charge to "MIT" as referring to actions by members of the community, including actions by students and faculty, as well as the decisions taken by MIT officials. We highlight some of MIT's actions at various points in Parts I, II, and III, and we note alternatives that might have been taken, but we do not attempt to judge whether some alternatives might have been preferable. We also indicate the questions in Part V that arise from the options we have identified.

IV.A The Investigation and the Immediate Post-arrest Period

MIT's involvement began with the observed September and October 2010 downloading events, of which it learned through emails from JSTOR asking the Institute to identify the perpetrator and stop the excessive downloading. JSTOR initially approached this downloading by blocking IP addresses, hoping that—as had been its previous experience—the incident would not recur. MIT was unable to use its "Stopit" procedure, as the perpetrator or perpetrators had registered with an anonymous email address. Shortly thereafter, MIT designed eControl to prevent future anonymous downloading, but—at the request of JSTOR—the mechanism was not implemented until January 2011—which, as matters developed, was too late.

IV.A.1 Locating the laptop and performing a packet scan

Given the scale of the downloading, its recurrence, the impact on JSTOR servers, and the concern that a significant portion of the JSTOR library was being copied (possibly for redistribution), identifying the downloader became imperative both to MIT and to JSTOR in order to stop the excessive downloading. The fact that the laptop registration was anonymous—and thus the owner could not be contacted—made it necessary to physically locate the laptop in order to identify what was happening.

IS&T could have simply unplugged the laptop and waited for someone to claim it, rather than performing a packet scan, which is an intrusive operation. In this case, the laptop was attached to the network in a nonstandard way, hidden from view in a closet, and performing possibly unknown operations for an unknown purpose. It thus seems prudent for IS&T to have attempted to capture and identify the network traffic. IS&T, as a network provider, is permitted to engage in such monitoring, but IS&T policies do not

seem clear about when such monitoring can be done, or how to treat the information that is collected. Part V, Question 2, suggests that these policies may be in need of review.

In light of the potentially serious consequences of the downloading to JSTOR, and thus to MIT, its licensee, and the persistent means whereby the perpetrator avoided the September and October attempts to terminate the activity, we find no other options to analyze that would enhance MIT's understanding and learning with regard to this stage of the investigation.

IV.A.2 Informing the MIT Police and notifying the Cambridge Police

IS&T could have attempted to deal with the discovery of the laptop on its own, without choosing to inform the MIT Police. However, a laptop attached to the network has the potential to perform a wide range of activities, and the MIT network has access to many services and databases that are critical for MIT research and education, some that involve sensitive information and government applications. Where an unknown individual or group has been actively engaged in accessing the network for several months, evading MIT's attempts to stop their observed downloading activities, and possibly engaging in other, unobserved conduct, it appears appropriate for IS&T to have asked for the MIT Police to become engaged immediately upon discovery of the foreign laptop attached to the network in a basement closet.

The MIT Police do not have expertise in computer or Internet crimes, nor do they have the ability to collect fingerprints or engage in the detailed analysis of evidence. It is standard practice for police departments to rely on other police departments when expertise is needed and not available; and it is standard practice for the MIT Police to contact the Cambridge Police under such circumstances. The fact that the MIT Police lacked the resources—and therefore lacked the option to conduct a more thorough investigation on its own—is an issue we raise in Part V, Question 1.

IV.A.3 Providing information to law enforcement pre-subpoena

As detailed in Appendix 7, some information generated during the downloading episodes was held beyond the length of time that MIT's internal policies permitted (absent specific authorization from OGC), and some information was provided to the USAO before a subpoena was issued. Initially, OGC approved the production of information to law enforcement, without a subpoena, as part of a continuing investigation of an ongoing intrusion into MIT's network as well as of a possible crime being committed on the MIT campus. IS&T continued to provide information to the investigators, pursuant to this initial approval, until OGC was eventually served with a subpoena on January 27, 2011.

In motions filed to suppress evidence, the defense claimed that some of MIT's actions in the gathering of information and its production to law enforcement violated federal law. As discussed in Appendix 10, our findings do not support such allegations.

A cursory examination of the statement of MIT policies on data retention and production indicates that they do not seem to be as clear or complete as they might be. Moreover, the interpretation of these policies could even be the subject of legal disputes, as was the case here in the motions to suppress evidence (see section III.D.2). Thus, a review of the Institute's data retention and provision policies seems desirable, as we suggest in Part V, Question 2. Increased MIT community awareness of these policies, and an understanding of the challenges of balancing the preservation of privacy and the need to maintain appropriate use of MIT's network, would serve as a learning opportunity for MIT more broadly.

With regard to the production of electronic data without a subpoena, IS&T consulted with OGC before providing any information to law enforcement; however, this request was made on January 4, 2011, when the laptop was first discovered and law enforcement was first called in. Thereafter, IS&T continued to follow OGC's initial guidance, despite a change in circumstances. This change was the result of law enforcement's commencement of a post-arrest investigation into Swartz's activities, an investigation no longer focused on what an unknown perpetrator was doing on the MIT network and what risk his conduct posed to that network, but focused instead on collecting sufficient evidence to prosecute and convict him. The laws concerning monitoring, capturing, and disclosing electronic communications for these two types of investigations are different. MIT's choice of actions during the post-arrest period complied with these laws (in the Review Panel's judgment—see Appendix 10), but compliance appears to have occurred only incidentally, as actions chosen without the benefit of expert advice to either IS&T or OGC. Early in the process, OGC had not yet arranged for an outside counsel with expertise in criminal law, and it never arranged for expertise regarding computer crime or electronic communications.

Part V, Question 1, asks whether, and how, that kind of legal and forensic expertise should be more readily available to OGC and to IS&T.

IV.B Neutrality: Issuing Statements; Providing Information to Prosecution and Defense

MIT chose to be neutral on the substance of the prosecution—it was neither in favor nor opposed as to whether Aaron Swartz should be prosecuted or whether, if charged, the charges should be felonies or misdemeanors. It conveyed that stance privately to both prosecution and defense. It chose not to issue public statements about the arrest, the prosecution, or the indictments. Overall, MIT sought to maintain the stance of a neutral

third party in a suit—*U.S. v. Swartz*—in which it was not involved. MIT had the options of stating its position publicly, of communicating different views either publicly or privately, and of communicating its views more strongly and persistently. The choice of substance and of method of its communications reflected multiple considerations, including: the fact that Aaron Swartz was not formally associated with MIT; MIT's appreciation of the significance of the allegations raised in its name against Aaron Swartz; and the extent of consultation between and among OGC, the Institute's administration, and the Institute's faculty.

MIT's stance on whether or not to issue statements, and, more generally, its choice of limited involvement, was reviewed on multiple occasions, and could have been changed at any of several points in time. For our discussion in this section, we select occasions when the possibility of change was particularly salient.

IV.B.1 Issuing public statements about whether to prosecute

On July 19, 2011, when the indictment was unsealed, and after JSTOR had settled its civil suit with Aaron Swartz, JSTOR issued a statement that included:

> The criminal investigation and today's indictment of Mr. Swartz has been directed by the United States Attorney's Office. It was the government's decision whether to prosecute, not JSTOR's. As noted previously, our interest was in securing the content. Once this was achieved, we had no interest in this becoming an ongoing legal matter.

The wording, "no interest in" is a little ambiguous, interpretable as "not in favor of" but also as "being neither in favor of nor opposed to." MIT did not issue a similar statement, neither one expressing the neutrality that was its policy, nor one opposing a prosecution. Nor was a statement issued clarifying that MIT was not involved in the decision to prosecute. The time of JSTOR's statement was a particular opportunity for MIT to issue its own statement.

Earlier, in June 2011, MIT had commented to JSTOR on earlier drafts of JSTOR statements, including a possible joint statement (see section III.A.4). Ultimately there was neither a joint statement nor a separate MIT statement. The time during which discussions with JSTOR about such statements were ongoing was also a time when it was apt for MIT to consider in depth its limited involvement. In addition to trying to influence the prosecutors (which might have helped or hurt Aaron Swartz), a public statement could have clarified MIT's position for both the MIT community and the public at large, even if it just presented the neutrality stance.

Public statements opposed to prosecution could have been issued at any time, and not just institutionally but by individual members of the MIT community. As noted in the

discussion of previous events (Appendix 9), the actions of individual members of the MIT community have made a difference in the past. Considerations that went into MIT's decisions to remain neutral relative to whether there should be a prosecution included a judgment of whether such statements would be helpful to Aaron Swartz, or whether they risked making matters worse for him. There was also a wide range of attitudes within the MIT community toward Aaron Swartz's actions on the MIT network. Even among MIT's proponents of open access (and among Aaron Swartz's friends), there was a general agreement that he had done something wrong. A blanket statement opposing prosecution could have been perceived as extreme by many in the MIT community. Beyond that, a position opposed to any prosecution at all could have been interpreted by many people as saying that MIT was uninterested in respecting its contractual agreements with licensors and was not serious about maintaining the integrity of its network.

IV.B.2 Issuing public statements about the criminal charges

Separate from neutrality toward whether there should be a prosecution at all is the role of neutrality toward the particular charges. Aaron Swartz was charged with felonies, not misdemeanors. Plea bargains offered by the prosecution included admitting guilt to felonies and risking jail time. An alternative option to a statement opposing prosecution per se (see section IV.B.1) was one that opposed specifically felony prosecution. As the felonies related to MIT's rules about access, MIT was intimately involved in the definition of the alleged crime and would eventually have been drawn into the discussion had there been a trial. As with section IV.B.1, public statements could have been issued at any time, and not just institutionally. Beyond the issues raised in section IV.B.1, this links also to the issue raised in Question 5 in Part V of MIT's institutional interests in the debate over reforming the Computer Fraud and Abuse Act.

IV.B.3 Making private statements to the prosecution about the criminal charges

MIT communicated its view on the prosecution and punishment to the USAO through OGC in the spring of 2011 and again through its outside counsel in August 2012. (See section III.C.3.) The questions of further pursuing private statements to the USAO and of altering the message being delivered arose particularly when two MIT faculty lobbied for more support for Aaron Swartz (see section III.C.5) and when defense counsel approached MIT about a joint meeting with USAO (see section III.D.1). OGC was willing to participate in such a meeting, but was not willing to significantly change its message to USAO—a message that remained in substance essentially neutral.

Central to this option would be abandoning neutrality and choosing to argue that it would be better to pursue misdemeanor charges rather than felony charges (and argue for dropping the demand for jail time and a felony record from plea negotiations). The

statements the Review Panel solicited from the two faculty members who argued for change from neutrality provide some reasons for taking such a stance.

We note that JSTOR made public statements and also private communications to the USAO regarding its attitude toward the prosecution (see Part II.C). The private communication appears to have been worded more strongly in support of Aaron Swartz than was its public statement. OGC was not aware of this private communication to the USAO.

As with the possibility of a public statement on the charges, considerations that went into the decisions to remain neutral in private statements at these times included judgments about whether such statements would be helpful to Aaron Swartz. Given the lead prosecutor's comments to MIT's outside counsel (see section III.C.3), MIT statements would seemingly have had little impact, and even risk making matters worse—although this information was not shared with Swartz's advocates.

IV.B.4 Providing prosecution and defense with documents and access to MIT employees

Section III.A.3 pointed out that "neutrality" can be viewed differently by different observers. A complication comes from the lack of symmetry in the abilities of prosecution and defense to obtain information for litigation purposes, as spelled out in Appendix 13, which reviews the legal structure of preparing for and proceeding with a trial. Thus, neutrality in the discovery context can be thought of in terms of acting similarly in responses to requests from prosecution and defense, or neutrality can be thought of in terms of acting to ensure equality of outcomes by offsetting the asymmetries in legal structure. As mentioned, at a time when the prosecution can produce a subpoena but the defense as yet cannot, responding similarly to subpoenas from each side is not the same as giving both sides equal access to information.

In the main, MIT acted neutrally in response to procedure, rather than to outcome. It could have done more for the defense. For example, it could have automatically supplied the defense with a copy of every document supplied to the prosecution, rather than waiting for a defense subpoena. Similarly, it could have offered a defense interview with every employee interviewed by the prosecution. The choice not to do this was based on a judgment that the criminal process was sufficiently fair, without the need for it to provide equality of outcome.

With the filing of the motions to suppress, in October 2012 the defense had placed itself in the position of alleging wrongdoing and illegal conduct on the part of MIT; and the role of the prosecution included rebutting any such allegations. This further asymmetry

between the roles of the prosecution and the defense led to an alteration of MIT's general stance toward true procedural neutrality, as described in section III.D.3.

Questions 7 and 8 in Part V situate these considerations on neutrality in making statements and providing information within a context of wider awareness of issues and attitudes. As these issues affect much of the MIT community, there is reason for a wide-ranging discussion.

IV.B.5 Taking non-neutral positions for people with MIT associations

When the Media Lab Director wrote to the administration in June 2011 (see section III.B.1), he asked whether MIT could consider this a "family matter." Others have suggested that Aaron Swartz could have been regarded as a member of the MIT community, based on the fact that he was a regular visitor to the MIT campus, interacted with MIT people and groups both on campus and off, and had made technical contributions to the World Wide Web Consortium, an organization hosted by MIT. The suggestion was that MIT should mitigate its neutral stance and advocate that the prosecution should reduce the severity of the threatened punishment.

In considering whether to maintain MIT's neutrality position, OGC, and the faculty members and others it questioned about this, began by asking whether Aaron Swartz was an MIT student. Upon learning that he was not, most of the people consulted agreed that staying neutral was appropriate. Similarly, Aaron Swartz's arrest and prosecution sparked little reaction from the MIT community, including students, which stands in marked contrast to previous incidents where students have gotten into legal trouble.

The limited extent to which the "core" MIT community engaged in discussion with the administration about the ongoing case, and the range of perceptions of the MIT community as to who is part of it for various purposes, concern two of the questions in Part V: whether to hold a community-wide discussion of the role of hacking as a legitimate part of MIT culture (Question 8); the nature of the obligation of MIT to its "greater" community (Question 7); and the extent to which MIT should intervene with law enforcement, even in the case of registered students accused of illegal activity. While we do not expect a consensus to arise from such discussions, it should lead to greater awareness of the views held across the community.

IV.B.6 Becoming more informed about the charges

OGC asked MIT's outside counsel for background understanding of the details of the indictment (and so of the role of the Computer Fraud and Abuse Act) late in the summer of 2012 and received a brief sketch of issues. Members of the MIT community who have been active in considering the CFAA did not draw the attention of OGC or the

administration to issues around CFAA during the prosecution. MIT had the option of exploring the charges earlier and considering the CFAA more broadly as part of formulating its responses to requests about statements. One particularly pertinent moment was in June 2011 when the Media Lab Director informed the administration that Aaron Swartz was charged with "unauthorized access" and suggested that MIT would be in a position to cast doubt on this charge if so desired (see section III.B.1). Other pertinent times were when the two federal indictments were issued, although the Review Panel does not suggest that it was MIT's role to offer lines of argument for the defense or to point out issues with the indictment. Similarly, members of the MIT community who were following the prosecution could have explored and discussed this issue in more detail.

A charge of "accessing [the MIT network] without authorization or in excess of authorized access" deeply involves MIT, since MIT provides the authorization and sets the rules of authorization. Thus MIT set rules that played a key role in determining what constituted a felony in the Aaron Swartz case. In the 1994 prosecution of David LaMacchia, MIT communicated to the USAO that, as a student, LaMacchia was authorized to access the computer as he had done. There was no reflection on the LaMacchia case during Swartz's prosecution: institutional memory had been lost. Part V, Question 1, in considering the need for greater expertise at MIT relating to computer crime, also asks about ways to help preserve institutional memory.

IV.B.7 Engaging more deeply with issues around the Computer Fraud and Abuse Act

As we are finishing this report, a bill has been filed in Congress to reform the CFAA, and dubbed "Aaron's Law." No doubt there will be extensive discussion before there is any legislation. MIT's roles, both in having chosen the rules and in interpreting their applicability to Aaron Swartz, make it clear that MIT has a real interest in contributing to the discussion. As MIT is a leading institution concerned with computers and network technology, MIT scholars and MIT institutionally have a role to play in encouraging reform. Thus, beyond the issue of exploring the charges against Aaron Swartz (based on wire fraud as well as access rules) earlier and in more detail, Question 5 in Part V raises the issue of MIT's general institutional concern with the CFAA.

PART V: QUESTIONS FOR THE MIT COMMUNITY

Question 1: *Should MIT develop additional on-campus expertise for handling potential computer crime incidents, thus giving the Institute more flexibility in formulating its responses?*

Question 2: *Should MIT policies on the collection, provision, and retention of electronic records be reviewed?*

Question 3: *Should an MIT education address the personal ethics and legal obligations of technology empowerment?*

Question 4: *Should MIT increase its efforts to bring its considerable technical expertise and leadership to bear on the study of legal, policy, and societal impact of information and communications technology?*

Question 5: *What are MIT's institutional interests in the debate over reforming the Computer Fraud and Abuse Act?*

Question 6: *Should MIT strengthen its activities in support of open access to scholarly publications?*

Question 7: *What are MIT's obligations to members of our extended community?*

Question 8: *How can MIT draw lessons for its hacker culture from this experience?*

Part V: QUESTIONS FOR THE MIT COMMUNITY

We have described the events concerning Aaron Swartz and his prosecution and MIT's involvement in those events. We now reach the portion of President Reif's charge that is, perhaps, the most important: discussing how we might learn.

Here in Part V we pose questions for the MIT community, and offer suggestions for how to address some of them, in the hope that doing so will aid the process of learning from this heartbreaking history. In selecting our questions, we draw on past incidents at MIT as well as the immediate one, and focus on structural issues raised by these experiences.

MIT's response to Aaron Swartz's arrest and prosecution reflected the MIT community's overall sentiment—a limited interest, as demonstrated by virtually the entire MIT

community. Before Aaron Swartz's suicide, the community paid scant attention to the matter, other than during the period immediately following his arrest. Few students, faculty, or alumni expressed concerns to the administration. Those most familiar with Aaron Swartz and the issues that greatly concerned him were divided in their views of the propriety of his action downloading JSTOR files, and fearful of harming his situation by taking public or private stands.[1] As strongly as we now wish, in hindsight, that events had turned out differently, and as we reflect on how MIT might have behaved differently—how *we* might have behaved differently—we recognize that we cannot and never will know whether *any* different actions on the part of MIT would have averted this tragedy. However, what we can do constructively now is to translate this tragedy into awareness and learning, procedures and actions that will help MIT become more like the community we strive to be.

The Review Panel was not asked to make recommendations in our report, but rather to suggest how MIT might learn from this history. In response, we offer several questions for the community to reflect upon, and some suggestions for a learning process. Some relate directly to the events described earlier in the report. Others are prompted by more general concerns that emerged in our interviews with faculty, administration, students, alumni, and knowledgeable outsiders, and reflections on MIT's responses to previous analogous events.[2] Some are mundane—significant although technical in nature; others are more philosophical, based on the morality a great institution must express and aspire to. We pose these as questions for deliberation by the entire community, not only by the administration and not only by the faculty, because it is as a community that MIT must answer them.

Question 1: *Should MIT develop additional on-campus expertise for handling potential computer crime incidents, thus giving the Institute more flexibility in formulating its responses?*

We raise this question relative to two areas of expertise: police expertise in computer issues and legal expertise in computer crime matters. When outside law enforcement (city, state, or federal) is involved on campus, MIT may have a diminished flexibility in choosing actions and approaches. The narrative in Part I shows how a decision to seek help from local law enforcement can, without any intent to do so, summon federal investigators and invite federal prosecution. In the Swartz case, had the downloader been found to be an MIT student, MIT might well have wished to handle the incident internally, as a disciplinary matter and not a criminal one. Here, the Secret Service became involved before Swartz's identity and his student-nonstudent status were known.

---

[1] This is based on private communications from some of Aaron Swartz's friends.
[2] See Appendix 9.

One question is whether MIT Police capabilities should expand to include expertise in dealing with cybercrime. There are many law-enforcement situations where the MIT Police must turn outside for help. Yet, given MIT's exposure in the online world, the wealth of technical expertise available within the MIT community, and the growth of cybercrime as a national concern, it is arguable that law enforcement involving cybercrime incidents should be an area where MIT has its own special capabilities. If so, where should those capabilities reside?

There is also the question of legal expertise regarding cybercrime and related criminal matters. The Office of the General Counsel addresses many legal issues that arise in the functioning of MIT, helping members of the MIT community as well as MIT itself. Complex criminal issues arise infrequently, and issues involving computer crime, the privacy of electronic data, and requirements for the disclosure of electronic communications arise still less frequently. In the Aaron Swartz case, MIT employed outside counsel with some of the relevant expertise to help with planning and managing interactions with USAO and defense counsels. However, this did not occur until almost the time of the first indictment, and the initial cooperation with law enforcement, including the collection and production of electronic evidence, took place well before such outside counsel was retained. There was apparently no ready access to outside computer criminal law expertise in the rush of events the day the laptop was discovered. Would having outside counsel on retainer, rather than employed on a case-by-case basis, be worthwhile in responding more quickly?

Another observation is that, perhaps due to the passage of time, there was no awareness within OGC of MIT's experience with the David LaMacchia case in 1994, described briefly in Appendix 9, with which the Swartz case has important parallels. Would MIT's understanding of the significance of the charges filed be better served with the construction of an ongoing history of significant cases in which MIT has been involved, rather than relying solely on the institutional memory of its lawyers and administration officials? Could outside counsel on retainer, rather than employed on a case-by-case basis, help preserve institutional memory?

The Review Panel's charge was to examine this particular case, but we are well aware that some of the same issues could arise in other realms. For example, many MIT people work at the intersection of computers and biology. Complex laws frame biological and medical care research, and there are edges where researchers, including students, may be drawn to do things that may end badly. While we do not attempt to extend our inferences for computer issues to other areas, other people should address this as MIT goes forward.

Continuing beyond the specific case of Aaron Swartz, a discussion of the potential interactions between internal policing and external police is germane for other areas, for example, illegal drug use. While the specific issues are very different, perhaps MIT can

review its experience in that realm and look for lessons that may help with other areas. This includes considering the extent to which students ought to be protected from prosecution, both with regard to fairness and with regard to the experience, education, and development of the students. It also includes the feasibility of employing legal counsel as a "legal ombudsman," to advise students on issues concerning their research projects—both those authorized by their academic instructors and those "not."

Question 2: ***Should MIT policies on the collection, provision, and retention of electronic records be reviewed?***

MIT's provision of records as recounted above reveals some gaps in its policies and practices around electronic records. Records were given to the Secret Service and the USAO with the approval of OGC, but there seems to have been incomplete clarity between OGC and IS&T over exactly what had been approved, and how long that approval lasted. Some records were turned over prior to subpoenas being issued. Some records were retained longer than MIT's retention policy called for, and for some kinds of records there seems to be no explicit retention policy at all. In addition, Aaron Swartz's attorneys, in a motion to suppress evidence involving the electronic records, claimed that some of MIT's actions in information gathering and provision violated applicable law (see section III.D.3). Given the issues and ambiguities, a review of MIT's data retention and production policies for electronic records seems appropriate. This is not only to improve the policies, but also to make the community more aware of these rules and the tensions inherent in trying to set appropriate rules.

Question 3: ***Should an MIT education address the personal ethics and legal obligations of technology empowerment? Should it include understanding of the legal frameworks that govern technology innovation and exploratory behavior? Should it include awareness of the interest in policy questions that will arise in future work of many graduates?***

Aaron Swartz was not an MIT student. But he was like many MIT students in that he was brilliant, technologically empowered, impassioned, and willing to work at the frontier: the very qualities that we celebrate in the MIT culture and value as engendering innovation and entrepreneurship. Gifted young people can readily exploit the power of the Internet to accomplish world-class good—and also to get themselves into world-class trouble. Aaron Swartz did both. As with Question 1, these issues arise in a variety of settings, not just computers and the Internet.

Should an MIT education include the opportunity to reflect on the personal choices to be made in exercising such technological brilliance and power? Does MIT have a responsibility to better prepare our students to grapple with the ethics of the decisions they will face as they go on to design new technologies to be used in the world? Should

MIT provide opportunities for students to better understand how to deal with the consequences of their decisions, as part of their technology education? Should students learn about legal restrictions on and societal debates about conduct "at the edges"? Could this be another way for MIT to demonstrate leadership as an educational institution? How might MIT make progress on realizing this opportunity?

Question 4: ***Should MIT increase its efforts to bring its considerable technical expertise and leadership to bear on the study of legal, policy, and societal impact of information and communications technology?***

The director of a leading computer research center commented to a member of the Review Panel that if MIT had had a stronger academic program in Internet policy, then the Institute might have addressed the Aaron Swartz case from a broader perspective. Be that as it may, Aaron Swartz's suicide has embroiled MIT in an Internet uproar that the Institute did not anticipate and with which it is not well prepared to grapple as a legal, policy, or social phenomenon.

As one faculty member commented:

> MIT prides itself on innovation and orientation to the future, but in defending a culture of rule-defiance, it can sound highly traditionalist: "this is the way we have always done it." But as society at large evolves, traditionalist cultures have to adapt sooner or later. In this case the complication is that MIT itself has been the source of so many of the changes now washing back on it.
>
> A similar narrative applies here with regard to complex legal systems that attempt to regulate theft and misuse of information. There may be a lot of libertarian types at MIT and beyond who do not want these controls imposed by the politically and economically powerful, but they are fantasizing if they think the world at large can operate indefinitely on the traditional cultural principles of the Institute.
>
> We should create an MIT Law Center, resembling Harvard's Berkman Center or the Oxford Internet Institute. The lack of such a center at MIT, which prides itself on leadership in all things technological, is astounding. MIT has no choice but to develop a much more robust capacity to study and teach such issues, for its own good as well as for the greater good.

If MIT had had a locus of scholarly activity around issues of information access during Swartz's arrest and prosecution, one can imagine that there would have been more active participation by the community as events were transpiring, more appetite for engaging the larger issues the prosecution brought to light, and more recognition of MIT's opportunity and responsibility to play a leadership role. There are a number of options for

expanding such scholarly activity to be considered, beyond the law center mentioned in the quote above. Emphasizing leadership positions might not itself have made a difference in MIT's specific actions involving Aaron Swartz, but it very well might have highlighted the opportunity to make public statements about our position, or encouraged individual members of the community to speak out.

Question 5: *What are MIT's institutional interests in the debate over reforming the Computer Fraud and Abuse Act?*

Aaron Swartz's death has stoked the flames of widespread criticism of the Computer Fraud and Abuse Act (18 USC §1030), one of two criminal laws under which he was prosecuted. There has been increased publicity about CFAA prosecutions in many parts of the U.S., together with calls for reform and a bill introduced in Congress.[3] MIT—and indeed many universities—have at least two institutional and educational interests in this debate.

MIT's first interest flows from the CFAA's "exceeds authorized access" clause. Under this clause, accessing MIT's computer network beyond the bounds set by MIT for such access can be a felony. However, MIT is not a legislature: it does not hold open debates about how its Terms of Service (TOS) should be crafted, defined, provided with "safe harbors," and otherwise applied; and it cannot foresee how rapid advances in technology and social uses of technology may make its TOS obsolete, unclear, or a dangerous and unintended trap for the unwary. Does MIT want to be in the position of determining what is and is not a felony? The application of this clause can criminalize even minor violations of TOS, and expose violators to civil and criminal penalties. In an intensive environment of exploration, it is not uncommon for researchers to conduct experiments that arguably violate the broad terms of service often associated today with websites and services. As one example, research involving collection and analysis of data about Internet services is vital to scholarly understanding of this medium.[4] Moreover, the CFAA has the effect of transforming minor violations of very broad service terms from a contractual issue (often never intended to preclude research) into a potential federal felony. This creates a chilling effect on important research and puts MIT in the awkward position of determining what is a felony based on its choice of the terms in its TOS.

---

[3] Grant Gross, "Aaron's Law would revamp computer fraud penalties," IDG News Service, June 20, 2013, <http://www.networkworld.com/news/2013/062013-aaron39s-law-would-revamp-computer-271093.html>.

[4] Examples of such experiments are data mining investigations that collect information by scraping websites. One particular example (among many) was seminal research in online privacy performed by two undergraduates, demonstrating that information about a person's Facebook "friends" can reveal that person's sexual preference ("Privacy Vanishes Online," *New York Times,* March 16, 2009 <http://www.nytimes.com/2010/03/17/technology/17privacy.html>. Data to support this hypothesis was collected by scraping Facebook pages, which arguably violated Facebook's terms of service.

A second MIT interest is the CFAA's prohibition against "unauthorized access," which can be hard to apply clearly in the context of MIT's open network environment. There, the question of who is "authorized" can rest on details of MIT's internal policies, such as the 14-day limit on "guest registrations." Aaron Swartz's attorney claimed that his access was in fact authorized as a consequence of MIT's guest policy, an issue that presumably would have been argued at trial had the case reached there.[5] Assuming, for the sake of argument, that Swartz did violate MIT's guest policy by, for example, remaining on the system for 15 days rather than the "authorized" 14: is such a "violation" material, and should such a violation turn acceptable conduct into a felony? A similar issue arose in the David LaMacchia case (Appendix 9), where the USAO initially planned to charge Mr. LaMacchia with unauthorized access under the CFAA, but decided against that when MIT refused to support the unauthorized access interpretation applied to its student. University rules of access are not designed for the purpose of defining the predicates for criminal prosecutions. Forcing them into this role impedes the university's ability to support open access and innovation.

There are many voices currently weighing in on the debate over CFAA reform, and MIT's role as a technology leader gives it special status to explain the impacts of the CFAA on research and academic exploration. MIT can press for change without necessarily taking sides in all facets of the debate on alternative ways to do reform.

Question 6: *Should MIT strengthen its activities in support of open access to scholarly publications?*

Aaron Swartz's downloading of the JSTOR database may have been motivated by the ideal of open access to scholarly works. Many commentators on the Swartz case have criticized MIT for not taking this into account in responding to his prosecution, given that MIT is itself a leader in advocating for open access. Should MIT be doing even more in support of open access to scholarly publications? At present, the MIT Open Access Working Group[6] is considering possible proactive initiatives in light of recent push-backs, by some publishers, against open-access policies. These include publicly advocating pro–open access positions with professional societies, increasing MIT's support for open-access journals, and strengthening MIT's commitment to the Faculty Open Access Policy.

---

[5] "Defendant's Reply in Support of Motions to Suppress and Motions to Dismiss Counts 1 and 2 of Superseding Indictment," Case 1:11-cr-10260-NMG Document 87 Filed 12/03/12, available at http://ia600504.us.archive.org/29/items/gov.uscourts.mad.137971/gov.uscourts.mad.137971.87.0.pdf.

[6] New Open Access Working Group Formed, MIT Faculty Newsletter, March/April 2012, <http://web.mit.edu/fnl/volume/244/holton.html>.

Another role MIT might play is to lend its institutional support to the FASTR (Fair Access to Science and Technology Research) Act currently before Congress, and to similar legislation. MIT could play a special role in demonstrating the value of FASTR's call for computational analysis, by state-of-the-art technologies, of the results of government-funded research.[7] Such an initiative would align well with some of the "Big Data" activities now springing up on campus.

MIT might also assume a leadership role among research universities in responding to the White House Office of Science and Technology Policy directive of February 22, 2013, directing major federal agencies that sponsor research to develop plans to make the published results of government-funded research freely available to the public.[8] Given our expertise in scholarly publishing, repository development, and digital preservation, MIT could offer, perhaps in conjunction with others, to assist agencies in creating such plans. Going beyond this, MIT could seek to mobilize the Association of American Universities (AAU) and the Association of Public and Land-grant Universities (APLU) around an initiative (such as SHARE[9]) whereby providing public access to the results of university scholarly research becomes the responsibility of the university research community itself—thereby strengthening the partnership between those who create knowledge and the public that benefits from it. And MIT could use its prestige and influence to actively advocate for strengthening copyright law's exceptions and limitations in support of scholarly pursuits, including fair use for the purposes of teaching, scholarship, and research.[10]

Question 7: *What are MIT's obligations to members of our extended community?*

MIT maintains an open campus and an open network and benefits from both. In that context, how should MIT treat people who actively participate in the life of MIT but do not have a formal, official connection, i.e., people with different relationships to MIT than those of students, faculty, and staff? Several people we interviewed for this report were emphatic that Aaron Swartz was a member of the MIT community, citing his involvement with the World Wide Web Consortium and his participation in technical forums. Others said that he was not a member of the community, pointing to the fact that

---

[7] "FASTR Aims to Speed Open Access to Government-Funded Research," *Library Journal*, February 21, 2013, <http://lj.libraryjournal.com/2013/02/oa/fastr-aims-to-speed-open-access-to-government-funded-research/>. See also Fair Access to Science and Technology Research Act of 2013, <http://doyle.house.gov/sites/doyle.house.gov/files/documents/2013 02 14 DOYLE FASTR FINAL.pdf>.

[8] John Holdren, Office of Science and Technology Policy, Memorandum for the heads of executive departments and agencies, February 22, 2013, <http://www.whitehouse.gov/sites/default/files/microsites/ostp/ostp_public_access_memo_2013.pdf>.

[9] SHared Access Research Ecosystem (SHARE) Proposal, Assoc. of Research Libraries, <http://www.arl.org/publications-resources/2772-shared-access-research-ecosystem-share-proposal>.

[10] 17 USC 107

he was not a student. Others were not sure, but said that he was at least a member of an "extended community."

Aaron Swartz's father noted that, in his discussions with some MIT administrators, he was asked if his son was a member of the MIT community. When he explained that his son was not a student or staff member, he felt that these administrators assured themselves that MIT had no responsibilities to Aaron and gave no consideration to the idea that Aaron was part of MIT's larger community of scholars and scientists.

Do we need to broaden our understanding of what it means to be part of the MIT community? In the words of one faculty member interviewed:

> Besides its faculty, students, staff, and employees, MIT has through the course of its history welcomed into its midst many who have only peripheral connections to the Institute and a number who have no affiliation whatsoever. These "guests" come via various informal routes as observers in laboratories, visitors in hallways, auditors in classrooms, readers in libraries, and overnight lodgers. Not all are integral to what goes on here, and some have little more than nuisance value, but many are tolerated because as a group they form part of a rich subculture that makes this community unique in its receptiveness to intellectual content regardless of credentials, points of origin, or other conventional standards. It is a relatively loose, undocumented subculture, but almost everyone here recognizes its prevalence, and values it as part of the fabric of this great institution.

What institutional obligations does MIT have to members of its larger community? What is the nature and scope of those obligations? If Aaron Swartz had been an MIT student, MIT might very well have reacted differently to his prosecution, if only because the Committee on Discipline could be available as an alternative mechanism for handling transgressions and the Dean for Students might have entered, and possibly altered, the trajectory of events. Should MIT develop a formal recognition of "guests," contributors, and other participants in the academic life of MIT? Should such possible recognition be captured in policy, or should it be left to informal channels and community awareness? While differences will always exist, there remains a basic issue of how MIT should think about responses to members of a wider community—as the underlying mindset will affect actions, whether it is codified or not.[11]

---

[11] While this question can be considered part of Question 8, we think it useful to recognize the issues in this question, without having them overwhelmed by the related questions for full members of the MIT community.

Question 8: ***How can MIT draw lessons for its hacker culture from this experience?***

MIT celebrates hacker culture. Our admissions tours and first-year orientation salute a culture of creative disobedience where students are encouraged to explore secret corners of the campus, commit good-spirited acts of vandalism within informal but broadly—although not fully—understood rules, and resist restrictions that seem arbitrary or capricious. We attract students who are driven not just to be creative, but also to explore in ways that test boundaries and challenge positions of power.

There are multiple times in the narrative of our review where one might wonder whether some earlier process of discussion and education might have had a positive impact on actions and decisions. A similar thought comes when considering earlier experiences involving students detailed in Appendix 9. In particular, students, faculty, staff, and administration might all benefit from a discussion of the nature of a desirable hacker culture, recognizing both advantages and risks.

This raises the question of whether the MIT community is sufficiently aware of what the hacker culture is meant to be about, of the risks inherent in crossing lines as part of hacking, and the roles of faculty, staff and administration in responding to what might or might not be a hack. And we note that there has been a persistent undercurrent of concern over the past several years that MIT's hacking tradition is being vitiated by a perceived increasing tendency to interpret hacking as a criminal activity. Some of the concern stems from incidents in 2006–2008 where students engaging in "unauthorized access" to various areas of campus ended up in Cambridge District Court, charged with breaking and entering with intent to commit a felony (as Swartz initially was).[12]

Yet in the computer context, unlike as in the physical world, "unauthorized access"—ill defined as it may be—can be grounds for a major federal felony prosecution. For Swartz the end result was calamitous. The entire episode may create a chilling effect for those students contemplating exploits that may push the bounds of their and society's knowledge, but will also take them to places where conventional rules say they are not supposed to be—"coloring outside the lines" so to speak, punishable by criminal records rather than mere forfeiture of crayons.

How can we prevent a robust hacking tradition from becoming a casualty of the Aaron Swartz tragedy? Is MIT doing enough to help students when their investigations lead them into confrontations with powerful authorities or existing law? Do we distinguish adequately the different sorts of ways students get into trouble and respond

---

[12] See "Hacking Tradition Under Fire?," *The Tech*, February 5, 2008, <http://tech.mit.edu/V127/N66/hacking.html>; "Lawyer: Student in NW16 Basement Was 'Hacking'," *The Tech*, July 9, 2008, <http://tech.mit.edu/V128/N29/hacking.html>; and "DiFava, Pierce Discuss Hacking at EC," *The Tech*, November 4, 2008, <http://tech.mit.edu/V128/N53/difavapierce.html>.

appropriately? Are we misleading students and community members by advertising one kind of community and enforcing rules more appropriate to a different kind of community? Are faculty, staff, and administrators on similar wavelengths about the responses that are most appropriate? While an extended discussion will not lead to uniform views, it would be good to expand awareness of the range of views in the community.

More generally, has MIT become overly conservative in its institutional decision-making around these incidents? More than once in our interviews, the Review Panel heard members of the MIT community express a feeling that there has been a change in the institutional climate over recent years, where decisions have become driven more by a concern for minimizing risk than by strong affirmation of MIT values. Several people interpreted the Institute's response in the Swartz case in that light. And some critics have chided MIT for playing such a passive role when Swartz's actions were motivated by principles that MIT itself champions. Yet we think it is important to view this tragedy in light of a history that may not conform with a myth of a golden past. For this reason we have referred repeatedly to some prior experiences.

One distinguished alumnus said to us, "MIT seemed to be operating according to the letter of the law, but not according to the letter of the heart," even while he expressed his enormous respect for the MIT leaders who had to grapple with these decisions. Is his concern on target? MIT aspires to be passionate about its principles, but we must also behave prudently as an institution. Of all the decisions MIT's leadership must make, those that require negotiating a balance between prudence and passion are some of the most wrenching. How can we make those choices easier to confront?

A possible way to move forward would be to charge a committee, composed of students, faculty, staff, and policy-administrators, to organize a series of campus-wide deliberations around issues raised by this report. These issues might include (but should not be limited to): What is the MIT community, and who is in it? What responsibility does MIT have to advise and, at times, oppose laws and government when it sees implications adverse to MIT's purpose and scope of leadership? What lines must MIT's students be made aware that they should not cross, or at least be sternly warned that "there be dragons" beyond? Where does MIT draw the line between risk-avoidance, so as to protect its more parochial interests, and risk-assumption, to promote those things in which it is interested?

CONCLUSION

As the length of this report demonstrates, the narrative of MIT's involvement in the events around Aaron Swartz's arrest and prosecution is extensive and intricate. This Review Panel hopes that we have set out the history of events with sufficient detail, clarity, and objectivity so that readers can consider the range of options that MIT faced, recognize MIT's actual choices as made in the context of events, and draw their own conclusions. We have also suggested areas where the Institute might learn from these events, including through community discussion and self-examination. Some of the issues that MIT faces transcend the particular events involving Aaron Swartz, and reflect broader concerns that emerged during our investigations. These include:

- The challenges of preserving open environments and open access in a digitally connected world that is increasingly apprehensive about computer crime and information misuse
- The dilemmas that arise in responding to members of our community—and our extended community—whose exploits land them in legal trouble
- The responsibility to help brilliant and innovative students navigate the ethical choices that accompany their technical empowerment
- The opportunity to reinforce MIT's institutional leadership in information technology by increasing scholarship and expertise in information law and policy

The Review Panel encourages MIT's administration to take the occasion of this report to stimulate discussions across the MIT community about these issues and the others described in Part V.

In concluding this review, we recognize the desire for a simple take-away, a conclusion that "if MIT had only done *this* rather than *that,* things would have turned out OK." We can't offer one. There were too many choices, too many might-have-beens, too great an emotional shock, and a public response that has been supercharged by the power of the Internet, the same power that Aaron Swartz epitomized and that he helped to create. Even today, with the benefit of hindsight, we have not found a silver bullet with which MIT could have simply prevented the tragedy.

If the Review Panel is forced to highlight just *one* issue for reflection, we would choose to look to the MIT administration's maintenance of a "neutral" hands-off attitude that regarded the prosecution as a legal dispute to which it was not a party. This attitude was complemented by the MIT community's apparent lack of attention to the ruinous collision of hacker ethics, open-source ideals, questionable laws, and aggressive

prosecutions that was playing out in its midst. As a case study, this is a textbook example of the very controversies where the world seeks MIT's insight and leadership.

A friend of Aaron Swartz stressed in one of our interviews that MIT will continue to be at the cutting edge in information technology and, in today's world, challenges like those presented in Aaron Swartz's case will arise again and again. With that realization, "Neutrality on these cases is an incoherent stance. It's not the right choice for a tough leader or a moral leader."

In closing, our review can suggest this lesson: MIT is respected for world-class work in information technology, for promoting open access to online information, and for dealing wisely with the risks of computer abuse. The world looks to MIT to be at the forefront of these areas. Looking back on the Aaron Swartz case, the world didn't see leadership. As one person involved in the decisions put it: "MIT didn't do anything wrong; but we didn't do ourselves proud."

It has not been the Panel's charge for this review to make judgments, rather only to learn and help others learn. In doing so, let us all recognize that, by responding as we did, MIT missed an opportunity to demonstrate the leadership that we pride ourselves on. Not meeting, accepting, and embracing the responsibility of leadership can bring disappointment. In the world at large, disappointment can easily progress to disillusionment and even outrage, as the Aaron Swartz tragedy has demonstrated with terrible clarity.

APPENDICES

Appendix 1: LETTER TO THE MIT COMMUNITY FROM PRESIDENT REIF

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

L. Rafael Reif, *President*

January 13, 2013

To the members of the MIT community:

Yesterday we received the shocking and terrible news that on Friday in New York, Aaron Swartz, a gifted young man well known and admired by many in the MIT community, took his own life. With this tragedy, his family and his friends suffered an inexpressible loss, and we offer our most profound condolences. Even for those of us who did not know Aaron, the trail of his brief life shines with his brilliant creativity and idealism.

Although Aaron had no formal affiliation with MIT, I am writing to you now because he was beloved by many members of our community and because MIT played a role in the legal struggles that began for him in 2011.

I want to express very clearly that I and all of us at MIT are extremely saddened by the death of this promising young man who touched the lives of so many. It pains me to think that MIT played any role in a series of events that have ended in tragedy.

I will not attempt to summarize here the complex events of the past two years. Now is a time for everyone involved to reflect on their actions, and that includes all of us at MIT. I have asked Professor Hal Abelson to lead a thorough analysis of MIT's involvement from the time that we first perceived unusual activity on our network in fall 2010 up to the present. I have asked that this analysis describe the options MIT had and the decisions MIT made, in order to understand and to learn from the actions MIT took. I will share the report with the MIT community when I receive it.

I hope we will all reach out to those members of our community we know who may have been affected by Aaron's death. As always, MIT Medical is available to provide expert counseling, but there is no substitute for personal understanding and support.

With sorrow and deep sympathy,

L. Rafael Reif

Appendix 2: LETTER FROM HAL ABELSON TO THE MIT COMMUNITY

January 22, 2013

To the MIT community,

President Reif has asked me to lead a review of our involvement in the events that began in fall 2010, when the library system learned that large numbers of articles were being downloaded from JSTOR, up through Aaron Swartz's shocking suicide on January 11. Among the thousands of news articles and postings over the past week—many strongly critical of MIT—there was at least one comment that saw a glimmer of encouragement that the administration has assigned this task to a faculty member strongly identified with the ideals of free and open access to information on the Net, the same ideals that Aaron championed so passionately. I'm grateful and humbled by President Reif's expression of confidence, and I'll try to approach this review with fairness and with respect to Aaron's memory, to his family, and to our community.

This matter is urgently serious for MIT. The world respects us not only for our scholarship and our science, but because we are an institution whose actions are and always have been guided by the highest ideals and the most thoughtful judgment. Our commitment to those ideals is now coming into question. At last Saturday's memorial, Aaron's partner Taren Stinebrickner-Kauffman described his mental state: "He faced indifference from MIT, an institution that could have protected him with a single public statement and refused to do so, in defiance of all of its own most cherished principles."

I don't know—*we* don't know—if that's accurate or fair. But it demands our response. I hope this review can provide some insight into what MIT did or didn't do, and why.

The review will not be a witch-hunt or an attempt to lay blame on individuals. We don't know what we'll find as the answers unfold, but I expect to find that every person acted in accordance with MIT policy. More than that: they acted in the belief that their actions were legally and ethically proper.

In last Sunday's *Boston Globe,* distinguished MIT alumnus and former US Senator John E. Sununu writes:

> For its part, MIT is conducting the inevitable soul-searching internal investigation. New administrative policies and campus rules will be written in the soft tones of academic boilerplate. But a new policy handbook will not suffice. This is a crisis of values and judgment, and it requires a change in attitude, starting at the top.

To this point, MIT's administration has refrained from speaking about this matter publicly, out of its expressed desire to first have a full record of events via our report. But when the record is clear, we will all need to ask if Sununu's criticism is on target. Are we becoming a place that, in the words of legal scholar James Boyle, "confuses order with rectitude"? That's a question not only for MIT's leadership, but something we will all need to ask of one another—and of ourselves.

This is for later in the spring. For now we will start with a review that gives us a clear record of what happened; that's the review that President Reif has asked us to conduct. I hope the report can be ready in a few weeks.

There have been dozens of questions in the press and on the Net over the past week. But the most important questions are the ones that will come from the MIT community, because we are the ones who will be held to account. IS&T has created a web site at http://swartz-review.mit.edu where you can suggest questions and issues to guide this review and you can comment on the questions of others. Please remember that this is about the first phase only—questions about what happened and why. A second phase, where we all deliberate over implications, will follow.

Hal Abelson
Class of 1922 Professor of Computer Science and Engineering

Comment from Review Panel (July 26, 2013): As this letter shows, the Review Panel had expected that producing this report would take only "a few weeks," when it actually required six months. When we began our review, we severely underestimated the number of witnesses to interview and the number of documents to collect and study, as well as the complexity of assembling a coherent history from the multiple (and sometimes divergent) perspectives of the many people who were involved in these events over a period of more than two years.

Appendix 3: REVIEW PANEL MEMBERS

Professor Hal Abelson

Class of 1922 Professor of Computer Science and Engineering, Department of Electrical Engineering and Computer Science, MIT

Professor Abelson is Class of 1922 Professor of Electrical Engineering and Computer Science at MIT and a Fellow of the IEEE. He holds an A.B. degree from Princeton University and a Ph.D. degree in mathematics from MIT. He was winner of the 1995 IEEE Computer Society's Taylor L. Booth Education Award, the 2011 ACM Karl Karlstrom Outstanding Educator Award, and the 2012 ACM Special Interest Group on Computer Science Education Award for Outstanding Contribution to Computer Science Education. Abelson is co-chair of the MIT Council on Educational Technology, which oversees MIT's strategic educational technology activities and investments. In this capacity, he played key roles in fostering MIT institutional educational technology initiatives such MIT OpenCourseWare and DSpace. He co-authored the 2008 book *Blown to Bits*, which describes, in non-technical terms, the cultural and political disruptions caused by the information explosion. A leader in the worldwide movement towards openness and democratization of culture and intellectual resources, he is a founding director of Creative Commons, Public Knowledge, and the Free Software Foundation, and a former director of the Center for Democracy and Technology—organizations that are devoted to strengthening the global intellectual commons.

Professor Peter Diamond

Institute Professor and Professor of Economics, Emeritus, MIT

Professor Diamond joined the MIT faculty in 1966, shortly after receiving his Ph.D. from MIT in 1963. He has been President of the American Economic Association, of the Econometric Society, and of the National Academy of Social Insurance. He is a Fellow of the American Academy of Arts and Sciences and a Member of the National Academy of Sciences. He has written on public finance, social insurance, uncertainty and search theories, behavioral economics, and macroeconomics. In the area of social security, he has been a member of a number of panels for the U.S. government since 1974. He has consulted about social security to the World Bank and has written about social security in China, Chile, Germany, Italy, the Netherlands, Spain, and Sweden as well as the U.S. His recent books include *Saving Social Security: A Balanced Approach* (with Peter R. Orszag), *Reforming Pensions: Principles and Policy Choices* and *Pension Reform: A Short Guide* (both with Nicholas Barr), and *Behavioral Economics and Its Applications*

(edited with Hannu Vartiainen). In 2010, he was a co-winner of the Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel for analysis of markets with search frictions.

Mr. Andrew Grosso, Esq.
Andrew Grosso and Associates, Washington, D.C.

Mr. Grosso is the principal attorney of the law firm of Andrew Grosso & Associates in Washington, D.C. From 1983 to 1994, he served as an Assistant U.S. Attorney in the Middle District of Florida and the District of Massachusetts, and, in addition to his law degree, holds master of science degrees in both physics and computer science. He has served on the Criminal Justice Section Council of the American Bar Association (ABA), has chaired that Section's Committee on Science, Technology and Forensics, and has twice chaired the ABA's National Institute on CyberLaw. He has served on the Committee for the International Freedom for Scientists of the American Physical Society, and is the current chair of the Law Committee for the Association for Computing Machinery (ACM) and serves on the U.S. National Policy Committee of the ACM.

Staff to the Review Panel:

Mr. Douglas Pfeiffer
Assistant Provost for Administration, MIT

Mr. Pfeiffer served in various administrative positions at MIT before joining the Provost's Office in 2007.

Appendix 4: PROCESSES FOLLOWED IN PREPARING THIS REPORT

The Review Panel faced several complexities in preparing this report. One is the intense public interest and controversy surrounding the prosecution of Aaron Swartz. Another is that we were charged with reviewing MIT actions that included those of the senior administration and the Office of the General Counsel. Yet another is that some of the documents relevant to the report are covered by attorney-client privilege. This appendix documents the processes we followed in addressing these issues. We also provide information on the documents we examined and the people we interviewed.

4.A Criterion for Naming Individuals

The Review Panel realizes that there has been significant controversy surrounding the events described. We appreciate that many of the people involved have legitimate concerns about their privacy and their security, and we know that some have even been personally threatened. Consequently, our report generally does not identify individuals by name. Many of these individuals have already been identified in court filings and other public documents, and we are fully aware that their names are readily discoverable on the Internet. Even so, we see no need to further erode their personal privacy. So as a rule, people in this report are identified by their role or position rather than by name. There are a few exceptions:

- In cases where including their names makes the narrative more understandable, we've named public officials—such as prosecutors, detectives, federal agents, judges, or police officers whose role in the events has already been described in public court filings.
- For some people actively involved in the events described, such as defense counsels for Aaron Swartz, we have used their names with their permission to do so.
- We named some people, whose connections are only tangential to the events described in the report, without having sought permission.

4.B Documents Examined

We examined about 10,000 pages of documents in preparing this review. These include legal productions; electronic messages among individuals at MIT; and correspondence with JSTOR, Aaron Swartz's attorneys, and the USAO.[1]

4.C Process for MIT Privileged Documents

Some of the documents pertinent to our review were covered by MIT's attorney-client privilege, such as specific legal advice provided to MIT employees by the OGC, and advice provided to MIT by its outside counsel. Some are protected by the work product privilege, such as where MIT anticipated that it would be involved in litigation concerning the production documents and other matters pertaining to these events. In order to protect MIT's privileges, and to avoid the chilling effect a full disclosure of these communications might have for future deliberations on other matters, between and among MIT attorneys, employees, and officials, even the Review Panel members were not given unrestricted access to this information. Instead, MIT engaged the outside firm of Wilmer Cutler Pickering Hale and Dorr LLP to manage a disclosure process. The Review Panel provided a list of potentially pertinent documents to attorneys from Wilmer Hale, who worked with the Panel's attorney Grosso, who was also engaged by MIT to ensure that all necessary information was evaluated for the report and to determine which privileged documents should be disclosed to the rest of the Review Panel.

4.D People Interviewed

The authors interviewed approximately 50 people in preparing this report. We're grateful for their time and their willingness to participate. Interviewees included:

- Samuel Allen
- Tim Berners-Lee
- William Bowen
- Jeremy Feigelson
- Andrew Good
- Eric Grimson
- Kevin Guthrie

[1] There are other potentially relevant documents that we have not seen. For example, we did not have access to the communications between the USAO and the Secret Service special agents during the course of their investigation.

- Susan Hockfield
- Richard Holton
- Andrew Huang
- Joi Ito
- Chris Kaiser
- William Kettlewell
- Brian LaMacchia
- Lawrence Lessig
- Quinn Norton
- Elliot Peters
- Rafael Reif
- Israel Ruiz
- Harvey Silverglate
- Star Simpson
- Taren Stinebrickner-Kauffman
- Robert Swartz
- Robert Ullman
- Martin Weinberg
- Susan Whitehead
- Members of the MIT Office of the General Counsel, the MIT Libraries, MIT Information Services and Technology, and the MIT Police who were involved in the events around Aaron Swartz
- A few MIT alumni, selected by the Alumni Office
- Student representatives chosen by the MIT Undergraduate Association and the Graduate Student Council
- Unnamed friends of Aaron Swartz

4.E Review Process for Publishing This Report

As the report neared completion, the authors prepared confidential controlled drafts of the various parts. *Controlled draft* meant that any further proposals for changes were recorded. All decisions about accepting changes were at the sole discretion of the Review Panel.

The following people and groups were given access to the controlled drafts, and allowed to propose changes:

- *Factual reviewers:* MIT library staff, network staff, members of the OGC and MIT Police officers who were interviewed for the report. They saw only the sections for which they provided information. The purpose of their review was to check for factual correctness only, and proposed changes were allowed only for factual correctness.

- *General reviewers:* The entire controlled draft was given to a group of 10 General Reviewers, who were selected by the Review Panel. The purpose of their review was to check that the report was readable and responsive to the President's charge. They were able to suggest any changes they deemed appropriate, but all decisions about accepting changes were at the sole discretion of the Review Panel.

After receiving comments from the General Reviewers, the authors prepared the final report and delivered it to MIT's President, for release to the public. The document given to the President was digitally fingerprinted to ensure that the published report would be identical to what the Review Panel produced.

Appendix 5: TIMELINE OF EVENTS

September 24/25, 2010	Unknown guest obtains access to MIT's network and begins excessive downloading of JSTOR articles.
September 26, 2010	MIT Class C network access to JSTOR blocked due to excessive downloading.
September 27, 2010	MIT's access to JSTOR restored, although source of downloading was not determined.
October 9, 2010	All MIT access to JSTOR fully blocked due to excessive downloading.
October 12, 2010	MIT's access to JSTOR restored; still no determination of downloading source.
October 12, 2010	MIT Academic Council members informed of the downloading incidents at their regular weekly meeting.
December 26, 2010	JSTOR informs MIT that it has detected additional excessive downloading.
January 4, 2011	IS&T staff find a laptop wired to a network server located in a network closet in Building 16. Laptop is identified as the source of JSTOR downloading.
January 5, 2011	U.S. Attorney's Office (USAO) opens criminal investigation of the accessing of MIT's network.
January 6, 2011	Aaron Swartz is arrested in Cambridge.
January 14, 2011	Three MIT employees (two from IS&T, one from Libraries) are interviewed by an Assistant U.S. Attorney, a special agent of the U.S. Secret Service, and a Cambridge Police detective.
January 27, 2011	First grand jury subpoena is served on MIT.
February 4, 2011	MIT's first production of documents in response to the January 27, 2011, subpoena.
February 18, 2011	MIT's second production of documents in response to the January 27, 2011, subpoena.

February 28, 2011	MIT's third production of documents in response to the January 27, 2011, subpoena.
April 13, 2011	MIT's final production of records in response to the January 27, 2011, subpoena.
May 6, 2011	The lead prosecutor tells MIT's Office of the General Counsel (OGC) that Aaron Swartz rejected a plea offer, and the case would likely move forward as a felony charge.
June 3, 2011	JSTOR settles its potential civil claims with Aaron Swartz.
June 6, 2011	MIT retains outside counsel experienced in criminal law.
June 13, 2011	Robert Swartz reaches out to the incoming Director of the MIT Media Lab, where he is a consultant, for assistance in dealing with MIT's administration and OGC on behalf of his son.
June 13, 2011	OGC responds via email to defense attorney William Kettlewell, informing him that MIT is not taking a position on whether Swartz should be prosecuted.
June 21, 2011	A conversation with the lead prosecutor leads OGC to infer that MIT's views on the case will have little impact on the prosecution going forward.
June 24, 2011	Second grand jury subpoena is served on MIT.
July 6, 2011	MIT's production of records in response to June 24, 2011, subpoena.
July 14, 2011	Federal indictment is returned and sealed.
July 19, 2011	Aaron Swartz voluntarily appears at the federal courthouse and is arrested.
July 19, 2011	The federal indictment is unsealed.
July 19, 2011	JSTOR issues a public statement disclaiming interest in further prosecution.
July 19, 2011	Demand Progress publishes article on Internet and solicits statements and signatures in support of Aaron Swartz.

September 14, 2011	Robert Swartz meets with MIT's Chancellor and an attorney from the OGC, and is told MIT's position is that of "neutrality."
October 25, 2011	Martin Weinberg takes over as Aaron Swartz's new defense attorney.
October 27, 2011	Andrew Good withdraws as defense attorney for Aaron Swartz.
November 6, 2011	State indictment issued.
March 8, 2012	State charges dismissed.
April 25, 2012	William Kettlewell and Martin Weinberg meet with MIT's outside counsel.
August 9, 2012	MIT's outside counsel speaks with the lead prosecutor, communicating MIT's positions on various issues concerning the prosecution of Aaron Swartz.
September 12, 2012	Robert Swartz again meets with MIT's Chancellor and an attorney from the OGC.
September 12, 2012	Superseding indictment is returned by a federal grand jury.
September 18, 2012	Eleven MIT employees (nine from IS&T, one from Libraries, and one from MIT Police) are interviewed by two Assistant U.S. Attorneys, a special agent of the U.S. Secret Service, and a Cambridge Police detective.
September 28, 2012	Martin Weinberg and William Kettlewell meet with MIT's Chancellor, General Counsel, and outside counsel, asking MIT to meet with the USAO in support of Aaron Swartz, and describing the motions they will file to suppress evidence, including that the motions will allege that MIT collected or produced information unlawfully.
October 5, 2012	Martin Weinberg files five motions to suppress evidence and one motion to dismiss the indictment.
October 16, 2012	Two MIT employees from IS&T are interviewed by two Assistant U.S. Attorneys and a Cambridge Police detective.
October 26, 2012	MIT's outside counsel notifies Martin Weinberg that MIT is willing to attend a meeting with the U.S. Attorney's Office, and of what MIT is willing to say, and not willing to say.

October 31, 2012	Martin Weinberg withdraws as Aaron Swartz's defense counsel.
November 6, 2012	Elliot Peters notifies MIT's outside counsel that Aaron Swartz's defense no longer seeks its participation in a meeting with the U.S. Attorney's Office.
November 8, 2012	Elliot Peters and Michael J. Pineault assume representation of Aaron Swartz in federal court.
November 16, 2012	Government files opposition to motions to suppress.
November 30, 2012	MIT receives a subpoena from Aaron Swartz's attorneys seeking documents.
December 11, 2012	Two MIT employees, one from MIT Libraries and one from IS&T, are interviewed by an attorney and an expert witness for Aaron Swartz.
December 14, 2012	A hearing on the previously filed motions to dismiss and suppress is scheduled for January 25, 2013.
January 3, 2013	Five MIT employees (three from IS&T, one from MIT Police, and one from Human Resources) are interviewed by two Assistant U.S. Attorneys and a Cambridge Police detective.
January 4, 2013	Four MIT employees (three from IS&T and one from Libraries) are interviewed by two Assistant U.S. Attorneys and a Cambridge Police detective.
January 11, 2013	Aaron Swartz, age 26, commits suicide in Brooklyn, New York.

Appendix 6: JSTOR AND THE MIT LIBRARIES

JSTOR (Journal Storage) is a not-for-profit organization that leases subscription-based access to digitized and digital versions of scholarly journals that span more than 50 disciplines in the arts and sciences. JSTOR's database currently contains over 1,400 journal titles from 800 publishers, and it has more than 10,000 institutional subscribers around the world. JSTOR's Scholarly Journal Archive provides nearly the entire run for each journal title, starting with its earliest issue. As an archive, JSTOR does not typically offer access to the most recent three to five years of a journal. JSTOR provides its journals under agreements with the original publishers, and copyright rests with the publishers, not with JSTOR. JSTOR was launched in 1995 with funding from the Andrew W. Mellon Foundation and with MIT as one of five charter institutional subscribers. JSTOR collections first became available in 1997.

MIT subscribes to nearly all of JSTOR's major journal collections. These journals are critical resources at MIT and at other research libraries. For MIT scholars, JSTOR is a main way to gain online access to the archival back runs of key scholarly journals such as the *American Journal of Mathematics*, *American Mathematical Monthly*, and *British Medical Journal,* and from key scholarly societies, including *Philosophical Transactions of the Royal Society of London, Science*, and journals published by the American Economic Association, the American Statistical Association, and the Society for In Vitro Biology. The MIT community uses JSTOR titles heavily. In 2012, about 130,000 articles were downloaded from the archive.

MIT's cumulative cost for JSTOR access since 1997 is approximately $620,000. This total includes an initial membership fee of approximately $30,000, followed by one-time (approximately $90,000) and ongoing leasing fees for each purchase of access to a collection, totaling approximately $60,000 per year. To put these numbers in perspective, purchasing subscriptions to hundreds of journals from a commercial publisher can cost more *each year* than the *cumulative* payments made to JSTOR since 1997.

Access to JSTOR's content, like most of the content MIT purchases for access through the MIT network, is offered under a license agreement between MIT and the content provider, and access is controlled through IP address recognition.

The access mechanism was changed in January 2011 in reaction to Aaron Swartz's downloading activities, as explained above in section I.E.2, *JSTOR and eControl*. Before January 2011, any computer on the MIT network could access JSTOR by simply going to http://www.jstor.org. Visitors to MIT could establish a guest account on the MIT network and access JSTOR by connecting their computer to the MIT network, as Swartz did.

From off-campus, members of the MIT community could obtain JSTOR articles by presenting their MIT-issued computer credentials, which let them connect to the MIT network via a VPN (virtual private network) or use the MIT Libraries' shortcut URLs to gain access through a proxy server.

Since early January 2011, access to JSTOR, regardless of the user's location, requires both the same MIT credentials that allowed off-campus access in the past, and an additional authentication check with MIT's human resources database. People using guest accounts can no longer access JSTOR articles, although visitors can still gain access through certain workstations located in the Libraries.

JSTOR's license agreement with MIT requires that MIT "shall use reasonable efforts to protect the Database from any use that is not permitted under this Agreement, and shall notify JSTOR of any such use of which it learns or is notified." It stipulates that the following activities are not permitted: using "Materials in a manner that would infringe the copyright therein" or "copy[ing], download[ing], or attempt[ing] to download an entire issue or issues of a journal from the Database."

As noted above, the MIT community downloaded about 130,000 articles in 2012. In 2010 and 2011, the respective download numbers were 5,329,326 and 567,488; the MIT Libraries' analysis indicates that the elevated numbers result from Aaron Swartz's download activity. Omitting the months when Swartz was downloading (and substituting average data for those months), the adjusted numbers are 228,919 for 2010 and 126,000 for 2011. It seems plausible that the drop in "actual" downloads between 2010 and 2011–2012 is due to the more stringent access controls that deny access to anyone not identified in MIT's human resources database as faculty, staff, or student.

Appendix 7: RECORDS PRODUCED BY MIT TO LAW ENFORCEMENT

During the morning of January 4, 2011, before the owner of the laptop had been identified, the U.S. Secret Service special agent asked MIT IS&T for whatever electronic records MIT might have that would be useful to the ongoing investigation. (See section I.B.) IS&T, after consulting with the Office of the General Counsel, turned over some records that same afternoon. These records were in the following categories: network flow data logs; DHCP server logs; RADIUS server logs; portions of the network registration database; and packet stream data. No subpoena had been issued to MIT at this point in time.[1] This appendix gives details and technical background on the electronic records provided and the relevant MIT policies. Appendix 10 provides a legal analysis of MIT's provision of these records.

7.A Network Flow Data Logs

Network flow data is collected by IS&T as part of routine network management, and the logs are retained. These logs show which IP addresses communicated with which other IP addresses; when the communication took place; how many bytes were transmitted; how many data packets were transmitted; and the network ports used. The logs do not contain the substance of the communications transmitted between IP addresses.

MIT IS&T's policy is to retain network flow data for as long as its storage capacity allows, up to a maximum of 30 days. In the case of the request by the special agent made on January 4, 2011, network flow data going back only to December 14, 2010, was available, and it was this data that was provided by MIT to the Secret Service on January 4, 2011.

7.B Dynamic Host Configuration Protocol (DHCP) Server Logs

Every computer is attached or connected to a network through a *network interface.* The network interface is identified by name or label, which is known as its MAC address (see Part I, footnote 4 for an explanation). MAC addresses are typically denoted by sequences of six two-digit hexadecimal numbers separated by colons. An example is 00:23:5a:73:5f:fb.

A computer attached to a network also needs an IP address, which the network uses to route data to and from the computer. IP addresses are typically denoted by a sequence of four numbers between 0 and 255, separated by dots, as in 18.25.132.16.

---

[1] MIT was first presented with a subpoena on January 27, 2011.

While MAC addresses are determined by the physical hardware of the computer and assigned at the time of manufacture, IP addresses identify the port on the network where the computer is connected, and they are determined by the network to which it is attached. An IP address can be periodically changed by the network, and IP addresses can be reassigned as computers are removed or relocated on a network.[2]

Assigning an IP address to a computer can be accomplished in different ways. One is for the computer and the network to agree on a fixed or permanent address. This is called a *static IP address.* Alternatively, the computer can request the network to assign it a *dynamic IP address*, that is, an address that is subject to change, using the network's Dynamic Host Configuration Protocol (DHCP) service. This is a service that finds available IP addresses and assigns them as needed. Unlike a static IP address, the dynamic address can be different each time the computer reconnects to the network (such as when it is turned off and then on)—and can change as a computer moves from location to location. To obtain the dynamic address, the computer contacts the network's DHCP Server and presents its MAC address together with a human-readable name, called a *DHCP client ID*. DHCP requests and assignments are recorded in the server's *DHCP log*.

When the special agent asked IS&T for information on January 4, IS&T took selected portions of the DHCP logs going back to the original September incidents, and extracted all entries containing the word "ghost." Here is a typical entry:

> Sep 25 16:42:42 wall-street dhcpd: DHCPREQUEST for 18.55.6.215 from 00:23:5a:73:5f:fb (ghost-laptop) via 18.55.0.1

It shows the "ghost-laptop" machine with MAC address 00:23:5a:73:5f:fb connecting on September 25, with the assigned IP address 18.55.6.215.

There were no records in the extracted DHCP logs for late October 2010 through January 2011, which includes the period of the most downloading activity in December 2010. This is because Swartz had assigned the ghost-laptop machine a static IP address for those downloading episodes. Static addresses are not recorded in the DHCP log.

IS&T's policy is to retain DHCP logs for at most 30 days, so a record from September 25, 2010, should not have been available on January 4, 2011. Exceptions for longer retention periods can be made with the approval of the Office of the General Counsel. In this case, the relevant DHCP log excerpts were retained because of the activity being investigated in September and October, but approval from the OGC was not sought at the

---

[2] MAC addresses and IP addresses can also both be changed by the computer's user, as Aaron Swartz did. (See section I.A.)

time. Noting this, the Review Panel recommends that IS&T revisit MIT's records retention policies and practices to ensure that practice aligns with policy.

7.C RADIUS Server Logs

MIT's Remote Authentication Dial In User Service (RADIUS) controls access to various network services, like wireless (mobile) services or printing. The RADIUS server log records this activity. The RADIUS log has little information beyond the MAC address and IP address of the requesting computer (not even showing what service was requested). Here is a sample entry:

> Thu Jan 6 13:26:52 2011 : Auth: Login OK: [00-4C-E5-A0-C7-56] (from client 18.6.187.14 port 7 cli 00-4C-E5-A0-C7-56)

RADIUS logs were not used by IS&T in its fall 2010 investigation of the downloading episodes. However, the logs in principle could have provided useful information. IS&T therefore supplied RADIUS entries in response to the request of the Secret Service for relevant electronic records. While the request was made on January 4, 2011, the information was provided on January 25, 2011. The logs that were produced covered the day of January 6, 2011.

MIT does not have a formal policy covering the RADIUS logs. In practice they are treated the same as DHCP logs with 30-day retention, since the information they contain is similar.

7.D Network Registration Database

The network registration database contains the computer registration information provided by guests and others. After the first grand jury indictment on July 14, 2011, MIT received a request for the registration information pertaining to Gary Host and Grace Host, and MIT provided six registration records to the lead prosecutor on September 28, 2011. Here for example is one of the six records provided:

> '00235a735ffb',0,'visitor',NULL,NULL,0,0,'Gary Host','ghost@mailinator.com','','',
>
> NULL,NULL,5,'29-Sep-2010','','24-Sep-2010','22:46:19',0,'30-Sep-2010','12:57:46',182635

The record shows the registration system, on September 29, 2010, reprocessing a registration for the Gary Host computer with MAC address 00:23:5a:73:5f:fb that was made on September 24, 2010, with a registration to expire on September 30, 2010.

MIT has no specific policy governing registration database records.

7.E Packet Stream

The stream of data packets to and from the suspect computer was captured by the MIT network engineer and recorded on an MIT laptop. This was accomplished within the network, as mentioned in Part 1, without making physical connection to the laptop or to the cable connecting the laptop to the MIT network. The recorded streams consisted only of the data packets directed to, and originating from, that specific suspect machine. There were about 87 GB in all, consisting almost entirely of JSTOR articles in PDF format. The exception was a small amount of control information that would be visible to all machines connected to the same subnet.

A hard drive with the captured packets was given to the Secret Service special agent on January 25, 2011, in response to a request made by the Agent on January 24, 2011.

There is no explicit IS&T policy governing packet streams. Capturing them is a very rare occurrence: it had been done fewer than five times in the previous five years. Streams are never captured as part of routine maintenance, but only for investigation.

Appendix 8: MIT AND OPEN ACCESS PUBLISHING

MIT has a history of being an early innovator in support of open access to scholarship, research, and educational materials. These efforts are a direct outgrowth of MIT's mission to "advance knowledge and educate students in science, technology, and other areas of scholarship that will best serve the nation and the world in the 21st century," and to "working with others to bring this knowledge to bear on the world's greatest challenges." MIT's researchers were instrumental in the origin and development of the free software and open-source software movements, and in recent years, MIT has taken the lead with groundbreaking projects in four major areas related to open access publishing. Many of these efforts are described on the MIT Libraries Scholarly Publishing website (http://libraries.mit.edu/scholarly/), which emphasizes how authors can retain and use their rights so that work produced at MIT can be openly shared.

The four major areas include open educational resources, open institutional repositories, open access to scholarly publications, and massive open online courses.

8.A Open Educational Resources: OpenCourseWare

In 2000, when many universities were exploring how they could profit from selling their course material for distance learning, MIT faculty proposed making MIT's courses openly available on the web for free viewing and reuse from anywhere in the world, in order to advance knowledge and education worldwide. MIT's unprecedented launch of OpenCourseWare, or OCW, began with a first proof-of-concept in 2002 with funding by the Hewlett and the Mellon Foundations. Ten years later, 2,150 courses had been published at the (http://ocw.mit.edu/). Following MIT's launch, OpenCourseWare has been adopted so extensively that in 2008 a nonprofit organization called the OpenCourseWare Consortium was created to coordinate the efforts of over 250 universities and associated organizations, who collectively share more than 13,000 open courses. Course content is made available under an open Creative Commons license, to maximize the possibility for remixing and reuse.

8.B Open Repository Software: DSpace

In 2002, MIT Libraries partnered with Hewlett-Packard to release the first public version of DSpace (http://dspace.mit.edu) open-source repository software, which is used for storing, accessing, and preserving scholarly and educational digital content and making it openly accessible. DSpace software has become one of the main platforms for universities to provide open access to their dissertations, research reports, research data, and faculty articles. Approximately 1,400 universities and other organizations have adopted the DSpace software and are offering live repositories using it. MIT's version of

DSpace contains approximately 60,000 items authored at MIT, all openly available around the world. MIT consistently ranks at or near the top of repository rankings, which assess impact and openness through a variety of measures.

8.C Open Access to MIT Scholarly Publications

In 2009, the MIT faculty voted to make their scholarly articles openly available on the web through MIT's open access repository DSpace@MIT. In the first such all-institution faculty-wide vote in the U.S., the faculty established an Open Access Policy because they are "committed to disseminating the fruits of [their] research and scholarship as widely as possible." The policy followed a model first adopted at Harvard's Faculty of Arts and Sciences, which has subsequently been taken up at more than 20 other universities in the United States. Through their Open Access Policy, the MIT faculty have made over 8,800 articles—one-third of the research articles they have published since the Policy's inception—openly available to the world. These articles have been downloaded over 900,000 times and have been met with gratitude from a wide range of readers, including students and researchers in developing nations, journalists, independent scholars, patient advocates, and job seekers.

8.D Massive Open Online Courses: *MITx* and edX

In late 2011, MIT launched *MITx*, a not-for-profit online learning initiative that offers complete MIT courses in an interactive online learning platform, through open-source software. In the spring of 2012, MIT and Harvard jointly launched a broader initiative as an outgrowth of *MITx*, called edX, to offer free online courses to students around the world, as well as those on their own campuses. Since that announcement, more than 28 other colleges and universities have joined the edX consortium, and hundreds of institutions around the world have expressed interest in collaborating. About 50 courses are available to the world, with hundreds of thousands of individuals already participating.

MIT's and its faculty's efforts to launch and nurture programs that make MIT's research and teaching openly available have not emerged by accident. These programs reflect MIT's core mission and most deeply held values.

Appendix 9: SOME PRIOR RELEVANT INCIDENTS AT MIT

This appendix describes three prior incidents where the MIT community became embroiled in controversy related to hacking or other use of electronics. Unlike the situation with Aaron Swartz, these incidents involved registered MIT students. They provide relevant background, and they may hold lessons to consider when looking ahead.

9.A David LaMacchia (1994)

The first incident reaches back two decades. Like the Aaron Swartz case, it shows how easily events can escalate with Internet-related misdeeds when federal law enforcement becomes involved. It also offers an example of prompt attention by MIT to the issue of authorized access.

The LaMacchia incident began in November 1993, at a time when MIT Information Systems was cooperating with the FBI to investigate a case of individuals based in Denmark who were accessing MIT workstations to stage penetrations of U.S. government computers. During the course of the investigation, the FBI asked MIT if they knew anything about two particular workstations in the Student Center. MIT did not notice anything suspicious about them, but about a week later, some students reported that these supposedly idle workstations were running with a large amount of disk activity. Information Systems and Technology (IS&T) investigated, and discovered that MIT sophomore David LaMacchia had set up an open File Service Protocol (FSP) server, which was being used as a transfer bulletin board for computer games and other copyrighted software. At that point, IS&T responded to the FBI's earlier question.

LaMacchia might have been charged with criminal copyright infringement, but in 1994, copyright infringement was not a criminal act if there was no profit motive involved, and LaMacchia was not engaged in any for-profit activity. The Boston U.S. Attorney's Office initially wanted to charge him with exceeding authorized access under the Computer Fraud and Abuse Act,[1] the same act that Swartz was indicted under. But MIT refused to affirm that LaMacchia had exceeded authorized access: according to MIT policy, MIT students had full access to these workstations (including root access) and were authorized to make any legal nondestructive use of them. The relationship of Aaron Swartz's actions and a legal interpretation of his access to MIT's network is more complex.

LaMacchia was indicted by a federal grand jury in April 1994 for conspiracy to commit wire fraud. He brought a motion to dismiss. The case was decided in U.S. Federal District

[1] 18 U.S.C. §1030.

Court in December 1994,[2] with District Judge Stearns referencing the Supreme Court decision in *U.S. v. Dowling* to effectively rule that the wire fraud statute could not be used to prosecute copyright infringement, and the case was dismissed.

Subsequently, the fact that LaMacchia could not be prosecuted for criminal copyright infringement became referred to as the "LaMacchia loophole." Congress closed this loophole in 1997 with passage of the No Electronic Theft Act,[3] which modifies copyright law to include some forms of noncommercial infringement within the scope of criminal infringement[4].

Despite the 20-year gap, some of the same people were involved in the Swartz and LaMacchia incidents. The lead prosecutor in the Aaron Swartz case was Deputy Chief of the Criminal Division of the Boston U.S. Attorney's Office during the LaMacchia case, and he met at one point with LaMacchia's defense counsel. Also, Andrew Good, Aaron Swartz's initial defense attorney, was a member of the LaMacchia defense team.

The LaMacchia case attained national notoriety. It was not on the same scale as the Aaron Swartz case, but it did gain attention from Congress, and it prompted a change in U.S. law.[5]

The charges of unauthorized access that the USAO initially contemplated filing against David LaMacchia, and the actual charges of wire fraud filed against him, were similar to the charges filed against Aaron Swartz.[6] This observation was not made by MIT during the Swartz prosecution, and not brought to the attention of the USAO.

The Swartz and LaMacchia cases were separated by 20 years. Insofar as the Review Team has been able to determine, despite the similarities in the two cases, there was no institutional memory inside of MIT spanning these 20 years, and so no mention of David LaMacchia as a precedent in any deliberations around Aaron Swartz by the MIT administration or the Office of the General Counsel, and no discussion of MIT's attitude towards a charge of unauthorized access.[7] Part V of this report poses the question of what

---

[2] *United States v. LaMacchia*, 871 F. Supp. 535 (1994)

[3] See "NET Act," <http://en.wikipedia.org/wiki/No_Electronic_Theft_Act>.

[4] The No Electronic Theft Act (the "NET Act") amended the Copyright Act, making it applicable to the conduct in which LaMacchia engaged. It did not amend the Wire Fraud Act. The Review Panel has not examined the reasons as to why the prosecution chose to not pursue a charge against Aaron Swartz under the NET Act.

[5] "Student Accused of Running Network for Pirated Software," *New York Times,* April 9, 1994; "Judge Rejects Computer-Crime Indictment," *New York Times*, December 1, 1994, <http://www.nytimes.com/1994/12/31/us/judge-rejects-computer-crime-indictment.html?src=pm> <http://www.nytimes.com/1994/04/09/us/student-accused-of-running-network-for-pirated-software.html>

[6] For the initial Aaron Swartz indictment, the wire fraud charge was Count One; for the superseding indictment, it was Counts One and Two.

[7] OGC was established at MIT on January 15, 2007.

MIT might do to better preserve its institutional memory, in the hope of being better prepared for future challenges.

9.B Andrew Huang (2002)

The Microsoft Xbox was a video game console introduced in 2001. It was designed to run only particular software licensed by Microsoft, using cryptographic methods to implement this restriction. Microsoft's licensing revenue for the software subsidized the cost of the machine, thus making it a powerful computer at a low price. In 2002, Andrew "Bunnie" Huang, a graduate student working in computer design at the MIT Artificial Intelligence Laboratory (AI Lab), discovered how to bypass this restriction, and thereby make Xboxes usable as general-purpose computers, with potentially serious consequences for Microsoft's product plans.[8] Huang posted a description of the method in his blog.

Soon afterward, an engineer with the Microsoft Xbox team contacted Huang and asked him to remove the posting. Huang informed his advisor, who cautioned him that the posting might be a violation of the Digital Millennium Copyright Act,[9] and suggested asking MIT lawyers for help.[10] Huang asked, and the response he received was a letter stating:

> . . . the article is your personal work, and not part of your studies, research or other activities at MIT. . . . as an MIT lawyer, I am not able to provide you with any legal advice concerning it. . . .

Huang described the predicament to his advisor and some other faculty members at the MIT Artificial Intelligence Laboratory. One of them arranged for Huang to get pro bono assistance from the Electronic Frontier Foundation (EFF). The EFF attorney advised that, as a precautionary measure, Huang should emphasize the academic aspects of his work by rewriting it as a scholarly paper and sending this to Microsoft for approval (following DMCA guidelines) for publication. Huang wrote the paper, and the faculty who were advising him arranged to publish it as an Artificial Intelligence Laboratory Memorandum.[11] At the same time, they informally contacted Microsoft executives,

---

[8] Huang's method involved connecting a hardware probe to the Xbox board to read out the secret keys that needed to be presented by the licensed software to the Xbox processor. The fact that he was able to do this demonstrated an important security vulnerability in the Xbox.

[9] The Digital Millennium Copyright Act (DMCA), 18 U.S.C. §1201(a) criminalizes the production or distribution of technology designed to circumvent access control mechanisms.

[10] At this time, MIT did not have a General Counsel's Office. The lawyer contacted was one of MITs intellectual property counsels—a group that was part of the MIT Technology Licensing Office.

[11] A. Huang, "Keeping Secrets in Hardware: the Microsoft Xbox(TM) Case Study," MIT Artificial Intelligence Laboratory Memo 2002-008. See also "MIT student hacks into Xbox," *CNET News*, June 3, 2002.

alerting them to what was being planned and advocating that Microsoft approve publication as a demonstration of its support for scholarly research. Microsoft agreed, and the memo was published and presented at an academic conference. Huang later expanded his work into a book.[12]

In 2013, Huang released a free reprinting of his book in honor of Aaron Swartz. He also wrote in his blog:

> Aaron's treatment by MIT is not unfamiliar to me . . . . I still remember the crushing disappointment of receiving a letter from MIT legal repudiating any association with my work, effectively leaving me on my own to face Microsoft. However, in my case, the faculty of my then-lab, the AI lab, were outraged by this treatment. They openly defied MIT legal by publishing my work as an official AI Lab Memo, thereby granting me greater negotiating leverage with Microsoft. Microsoft, mindful of the potential backlash from the court of public opinion over suing an openly legitimized academic researcher, came to a civil understanding with me over the issue.[13]

This example points to the flexibility available without the presence of outside law enforcement. It also illustrates the point that when it is a student who has a situation like this, it naturally brings in additional members of the MIT community.

9.C Star Simpson (2007)

On September 21, 2007, MIT sophomore Star Simpson was arrested at gunpoint at Boston's Logan Airport. Simpson, who had gone to the airport to meet her boyfriend, entered Terminal C wearing homemade electronic jewelry: a lapel pin consisting of circuit board with flashing LEDs, which she had built in her free time, at the MIT Electronic Research Society club. Airport employees mistook this for a bomb and called airport security and the police. Simpson was accused of disorderly conduct and possession of a hoax device: a charge that could have resulted in up to five years in state prison.[14] Simpson was sentenced to pretrial probation and ordered to perform community service. The charges were eventually dropped.

On the same day as the arrest, before anyone in the MIT administration had spoken with Simpson, the MIT News Office issued a press release saying that "As reported to us by

---

[12] A. Huang, *Hacking the Xbox: An Introduction to Reverse Engineering,* No Starch Press (2003). See also J. Zhang, "XBox Security Key Finder To Publish Hacking Book," *The Tech,* May 9, 2003.

[13] A. Huang, "A moment of silence for Aaron Swartz," <http://www.bunniestudios.com/blog/?p=2860>.

[14] "MIT sophomore arrested for innocuous LED device," *The Tech*, September 25, 2007; also "MIT student arrested at Logan in bomb scare," *Boston Globe,* September 21, 2007.

authorities, Ms. Simpson's actions were reckless and understandably created alarm at the airport." Many members of the MIT community did not view Simpson's behavior as reckless. They were upset at what they regarded to be an unwarranted and prejudicial public statement by the Institute to the detriment of one of its members.

At the October 17, 2007, faculty meeting, several faculty members introduced for discussion a resolution proposing that "the MIT faculty request that the MIT administration refrain from making public statements that characterize . . . the behavior and motives of members of the MIT community whose actions are the subject . . . of pending criminal investigation." The resolution was taken up at the following December 19 faculty meeting. It was eventually voted down (31-36) after two hours of vehement debate, which included the offering and defeat of several alternative resolutions. In the end, none of the resolutions were adopted, but the intensity of the meeting made a lasting impression on the administration. At the May 2008 faculty meeting, President Susan Hockfield expressed regret over her administration's handling of the case. She stated that the administration regretted its public statement, that the decision to make the statement was rushed, and that it included a poor choice of words.[15]

These October and December faculty meetings, and the proposed resolution, were cited by the administration as part of the reasoning for not making a statement about Aaron Swartz. (See section III.A.3.)

[15] Record of the Meeting of the Institute Faculty of Wednesday, May 21, 2008, https://web.mit.edu/dept/libdata/libdepts/d/archives/facmin/071219/071219-minutes.pdf.

Appendix 10: LEGAL ANALYSIS OF MIT'S PROVISION OF DOCUMENTS AND PACKET CAPTURE

MIT engaged in its own investigation of the JSTOR downloading events, beginning in September 2010. MIT cooperated with law enforcement once it became involved, starting January 4, 2011. The purpose of this appendix is to provide some legal framework and analysis for the actions of MIT, regarding the capture and disclosure of electronic data.

On four separate occasions MIT produced electronic data to law enforcement regarding Aaron Swartz's use of the MIT network: (1) on January 5, 2011, prior to his arrest, it produced records concerning the downloading engaged in by Aaron Swartz, that is, "metadata"; (2) on January 25, 2011, it produced packet data, that is, electronic communications, including the articles downloaded by Aaron Swartz; (3) on May 6, 2011, it produced a CD with copies of the data already produced; and (4) in September 2011, it produced additional metadata. See the Report, I.B; Appendix 7. The third set of data was produced pursuant to grand jury subpoena; and the fourth was produced by MIT under the belief that it was responding to a valid subpoena (a belief that may not have been true). The analysis below indicates that all four sets of data were properly produced by MIT, although for different reasons.

10.A The Federal Laws Protecting Electronic Communications

The two federal laws governing the interception and disclosure of electronic communications are (1) the Electronic Communications Protections Act (ECPA), 18 U.S.C. § 2510 *et seq*.; and (2) the Stored Electronic Communications Act (SECA), 18 U.S.C. § 2701 *et seq*. As their names imply, they address, primarily, electronic communications in transit and electronic communications when they are stored.

10.A.1 The electronic communications were lawfully disclosed

ECPA defines an electronic communication very broadly.[1] It is:

> [A]ny transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . . .

[1] 18 U.S.C. § 2510(12). This definition includes several exceptions, which are left out of the quoted portion and do not concern this Report.

The JSTOR articles downloaded by Aaron Swartz were electronic communications. Arguably, the instructions communicated by his laptop to JSTOR's servers asking for these articles also fell within the scope of this definition.

ECPA prohibits both the "interception" of electronic communications and the disclosure of such intercepted communications, except under certain delineated circumstances. The prohibition against interception provides[2]:

> Except as otherwise specifically provided in this chapter any person who—
>
> > (a) Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . [is in violation of law].

The prohibition against disclosure reads[3]:

> [Whoever] intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection [is in violation of law];

A careful reading of both of these provisions reveals that their application depends upon the meaning of the words "intercept" and "interceptions." The term "intercept" is defined by ECPA as the "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[4] On the surface, this is a very broad definition of "intercept." However, two provisions appearing elsewhere in ECPA limit the applicable scope of this definition.

The first of these[5] allows the provider of an "electronic communications service" (such as MIT's network services) "whose facilities are used in the transmission of [an] electronic communication" to:

> intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service . . . .

---

[2] 18 U.S.C. § 2511(1)(a).
[3] 18 U.S.C. § 2511(1)(c).
[4] 18 U.S.C. § 2510(4).
[5] 18 U.S.C. § 2511(2)(a)(i).

Under this provision, the conduct of MIT's IS&T personnel during the period between the discovery on January 4, 2011, of the laptop in the network closet in the Dorrance Building and Aaron Swartz's arrest on January 6 comprised activity that was necessary to the "protection of the rights and property" of MIT's network. Thus, the monitoring and capture of communications flowing over the MIT network during this period, while in transit between Swartz's laptop and JSTOR's servers, was lawful.[6]

The second exception concerns the doctrine of one-party consent. ECPA permits a person, whether a law enforcement officer or otherwise, to intercept an electronic communication where one of the parties to the communication "has given prior consent to such interception."[7] Here, the discussions between MIT Libraries and JSTOR in the months leading up to the arrest of Aaron Swartz indicate that MIT had JSTOR's permission to intercept the articles being downloaded, and the accompanying electronic signals, in an effort to identify the perpetrator and to stop him.[8]

Since the interception of these communications was lawful, the prohibition against disclosure of intercepted communications did not apply: that prohibition only applies to the disclosure of communications obtained through an interception that is in violation of ECPA.[9] Electronic communications were produced by MIT to law enforcement on two occasions: packet data on January 25, 2011; and a copy of the packet data, on May 6, 2011. For the reasons here discussed, these productions were permissible under ECPA.

10.A.2 The metadata was lawfully disclosed

We now turn to SECA, specifically its provisions regarding metadata.

In substantial part, SECA protects electronic communications that have been stored.[10] These provisions are not at issue here, as the electronic communications produced by MIT to the government were not taken from electronic storage but were monitored and captured in real time on the MIT network.

---

[6] We take note of the fact that at no time did MIT "tap" into the cable connecting Swartz's laptop computer to MIT's network. Thus, all of the communications at issue were captured while flowing through the MIT network, and the exceptions to the prohibition found in ECPA as here noted apply.

[7] 18 U.S.C. § 2511(2)(d).

[8] As we noted above, JSTOR asked MIT to stop the downloading and instructed MIT as follows: "We are requesting that every effort be made to identify the individuals responsible and to ensure that the content taken in this incident and those previously mentioned is secured and deleted." See section I.A.

[9] 18 U.S.C. § 2511(1)(c).

[10] SECA is sometimes interpreted as applying to only communications being stored *pending* transmittal to the intended recipient and, once that transmission is accomplished, its protections no longer apply—even where a copy of the communication remains in electronic storage. *Jennings v. Jennings*, 401 S.C. 1 (2011), *cert. denied*, *Jennings v. Broom*, __ U.S. __, 2013 U.S. LEXIS 1301 (April 15, 2013).

SECA also addresses metadata concerning electronic communications, e.g., records of session times and durations, dates of commencement of communications, and network addresses. Similar to ECPA, SECA contains an exception to the prohibition regarding disclosure of the information that it covers, this being where the disclosure is necessary to protect the rights and property of the communications service provider.[11] The metadata produced to the prosecution before the arrest of Aaron Swartz falls into this scenario.

SECA also provides that records of electronic communications can be produced pursuant to a grand jury subpoena (and certain other administrative or judicial orders).[12] The copy of the metadata data reproduced in May 2011 falls under this provision, as MIT turned it over pursuant to the grand jury subpoena served on January 27, 2011.

However, as noted above, in September 2011, IS&T turned over additional network flow data concerning Aaron Swartz's downloads. This was done under the (possibly) mistaken belief that the January 27 subpoena was still valid and effective. Assuming for the sake of argument that this belief was wrong and the subpoena was no longer valid (see section 10.C below), MIT was nonetheless legally justified in disclosing these materials to the prosecution: a good faith reliance on the validity of a subpoena demanding records of electronic communications legally protects the service provider from a claim that it acted in violation of SECA.[13]

We also note that ECPA (18 U.S.C. § 2511(2)(h)) expressly allows a provider of electronic communication services to:

> [R]ecord the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

For these reasons, MIT was not prohibited by either SECA or ECPA from disclosing to law enforcement the metadata it collected.

10.B Massachusetts Law Regarding Electronic Communications

The Massachusetts Wiretap Act is worded somewhat differently than ECPA. It too allows a communications provider to intercept communications to protect the rights or property

---

[11] 18 U.S.C. § 2702(c)(3).
[12] 18 U.S.C. § 2703(c)(2).
[13] *Sams v. Yahoo!,* 713 F.3d 1175 (9th Cir. 2013). The Review Panel expresses no opinion as to whether the prosecution could introduce such material at trial if the January 27 subpoena was no longer valid at the time that the prosecution asked MIT for this information.

of such provider.[14] With regard to *subsequent* disclosure of a communication that has been intercepted—whether lawfully or unlawfully—such disclosure *is* a violation of the Act,[15] unless either: (1) it is "a necessary incident to the rendition of service or to the protection of the rights or property of the carrier of such communication . . ."; or (2) it is pursuant to a judicially issued warrant.[16] However, during the joint federal-state investigation of Aaron Swartz's activities concerning the MIT network, federal law—and not the Massachusetts Wiretap Act—applied to MIT, the Secret Service, and the Cambridge Police Department.

Where an investigation is primarily federal in nature, regardless of whether there is involvement by state or local law enforcement, the federal ECPA supersedes the Massachusetts Wiretap Act.[17] Where the investigation is joint in nature, but is primarily "state-oriented," then the Massachusetts Wiretap Act applies.[18] The critical fact that determines the nature of the investigation is not where the case is ultimately prosecuted (*e.g.*, in the federal or state court), but rather the nature and direction of the investigation at the time the conduct at issue occurs.[19]

Given the circumstances of the Aaron Swartz investigation, and the nature of the joint federal-state investigation and subsequent prosecution, federal and not state law applied to the interception and disclosure of Aaron Swartz's communications across the MIT network.

10.C Document Production

During the course of the investigation and prosecution of Aaron Swartz, MIT produced numerous documents, as well as electronic copies of the articles downloaded by Aaron Swartz from JSTOR. We take the opportunity to examine MIT's decisions regarding such production and law enforcement's use of its subpoena power.

Beginning on January 4, 2011, MIT's IS&T produced information to law enforcement. This was part of IS&T's own attempt to protect its network, and to assist law enforcement in doing the same. MIT's OGC was consulted by IS&T about the propriety of producing these materials, and OGC gave its approval. OGC's focus was on the following issues: (1) there was no personal identifying information in the material to be produced; (2) the perpetrator was misusing MIT's network, possibly committing a crime and injuring JSTOR, and MIT wished to cooperate with law enforcement.

---

[14] Mass. Gen Law. ch. 272 § 99(D)(1)(a).
[15] Mass. Gen Law. ch. 272 §99(C)(3)(a).
[16] Mass. Gen Law. ch. 272 § 99(D)(1)(a).
[17] *Commonwealth v. Gonzalez*, 426 Mass. 313 (1997).
[18] *Commonwealth v. Jarabek*, 384 Mass. 293 (1983).
[19] *See Gonzalez*, above.

After the arrest of Aaron Swartz, IS&T continued to produce documents to law enforcement without (initially) further consultation with OGC. Apparently, IS&T considered the initial advice provided by OGC to still govern, despite the fact that the situation had changed: MIT was no longer disclosing communications in an effort to protect its network, but to assist law enforcement in a possible criminal prosecution. Had MIT continued to intercept communications between JSTOR and the laptop of Aaron Swartz for more than an incidental period of time after his arrest, then this exception to ECPA[20] would not apply. However, the interceptions essentially stopped at this point as the laptop was removed from its connection in the SIPB office. Thus, all of these interceptions were lawfully obtained and disclosed.

In late January 2011, the prosecution served a grand jury subpoena on MIT seeking a large number of documents, and MIT produced documents and information pursuant to this subpoena. Thereafter, MIT insisted upon being served with a subpoena before agreeing to produce additional matter that it considered to be outside the scope of the initial subpoena.

Two grand juries appear to have been involved in the investigation and prosecution of Aaron Swartz: the first of which issued the two subpoenas and returned the initial indictment, and a second, which returned the superseding indictment.[21]

In September 2011, the prosecution asked for and received additional information from IS&T. This was produced by MIT under the belief that it was covered by the initial subpoena, served in January 2011. However, it is unlikely that this initial subpoena was still valid, in that the first grand jury had completed its work: it had returned its indictment and no evidence appears that it was continuing its investigation into additional crimes, additional defendants, or an expanded scope of the offenses already charged.[22] The prosecution did not notify MIT of this (apparent) fact. Thus, MIT, unknowingly and unintentionally, may have produced documents to the prosecution without benefit of a court order, that is, without benefit of a subpoena. As noted above, MIT's conduct in this regard was proper.[23]

---

[20] 18 U.S.C. § 2511(2)(a)(i); see also one-party consent doctrine discussed above.

[21] The Review Panel concludes that two grand juries were used from the following facts. First, the names of the foremen who signed the two indictments are different. Second, grand juries (usually) sit for only 18 months, and the time period between the issuance of the first subpoena from the (presumed) first grand jury, in January 2011, and the return of the superseding indictment, in September 2012, is some 20 months.

[22] As noted in Appendix 13, the prosecution may not use a grand jury to conduct additional investigation the purpose of which is to prepare for trial.

[23] *Sams v. Yahoo!,* 713 F.3d 1175 (9th Cir. 2013).

Appendix 11: COMMENTS ON THE COMPUTER FRAUD AND ABUSE ACT CHARGES AGAINST AARON SWARTZ

The way in which MIT's rules of access to its network interact with possible charges under the Computer Fraud and Abuse Act (CFAA) is an important lesson for MIT and is discussed in Part V of the Report. Here, we discuss the interaction of MIT's Rules of Use with the charges brought against Aaron Swartz, an interaction that would have been sorted out in the hearings or the trial, had they occurred.

The initial indictment against Aaron Swartz contained four counts, each alleging a different violation of law, i.e., a different legal theory. The superseding indictment took these four counts and the events described in them, "unbundled" these counts, and created 13 counts out of the initial four. Also, the theory of criminality in the last count was expanded.

We briefly examine those counts alleging violations of the CFAA as they involve MIT.

Count 3 of the initial indictment and counts 8 through 12 of the superseding indictment allege that Aaron Swartz "unlawfully obtained information from a protected computer." In this instance, the computers at issue are the servers at JSTOR and the network servers and routers at MIT, which are included as protected computers under the Act, inasmuch as they affect interstate commerce since they are connected to the Internet. In the superseding indictment, only counts 9 and 12 directly address MIT's computers, with counts 8, 10, and 11 addressing JSTOR's computers.

The initial indictment alleged that Aaron Swartz used two unlawful means of accessing these protected computers: through "unauthorized access," and by "exceeding authorized access." The superseding indictment abandoned the second legal theory. We take the time to examine both theories as they might have been applied to MIT.

The authorizing of "access" to a computer is made by the owner or administrator of the computer. Here, that would be MIT. The terms and conditions of that access are found in MIT's terms of service, known at MIT as "MITNet Rules of Use."

11.A Exceeding Authorized Access

The first request made by the government for the MITNet Rules of Use that were in effect during the period of excessive downloading was made by the lead prosecutor, by email, on July 28, 2011. This was almost two weeks after the first indictment had been returned. MIT produced them the same day. On August 4, the lead prosecutor asked MIT,

again by email, whether a link to the rules appeared on a guest user's registration page. MIT again responded the same day. The Rules of Use were:

1. Don't let anyone know your password(s).
2. Don't violate the privacy of other users.
3. Don't interfere with the integrity of the system.
4. Don't copy or misuse copyrighted material (including software).
5. Don't use the network to harass anyone in any way.
6. Don't restrict or deny access to the network by legitimate users.
7. Don't use the network for private financial gain.

The only Term of Use rule clearly applicable to Swartz's conduct was the fourth. However, inasmuch as MIT had held license from JSTOR for authorized users to copy JSTOR's articles, it appears open to dispute whether Swartz's conduct exceeded authorized access *on the MIT network*. (This analysis does not address issues of authorized access to JSTOR's network.) This was not a question raised or discussed by MIT, or brought to the attention of the USAO.[1]

Several other terms may appear applicable, such as:

> No. 3: "Don't interfere with the integrity of the system"; however, although Aaron Swartz clearly interfered with the integrity of the JSTOR system, he never interfered with the integrity of the MIT system, to which this term seems directed;[2]
>
> No. 5: "Do not harass"; however, harassment has an element of intent, and there is little indication that Aaron Swartz had as his purpose the goal to harass anyone; and
>
> No. 6: "Do not deny the system to other users"; however, although it is true that for two brief periods of time JSTOR cut off the MIT campus from its services in response to the massive downloading, here Aaron Swartz did not himself deny or intend to deny the system to other users.

---

[1] We again note that the superseding indictment, returned in September 2012, eliminated "exceeding unauthorized access" as the basis for any of its counts. In view of JSTOR's terms of service, the Review Panel makes no findings as to whether Swartz's conduct exceeded authorized access on JSTOR's network.

[2] We note the Doctrine of Lenity, discussed in Appendix 13, which requires the application and interpretation of criminal laws to be narrowly drawn and, where ambiguous, in favor of the defendant.

The Review Panel draws no conclusion as to whether Aaron Swartz did or did not exceed authorized access on the MIT network. We also remark that, consistent with its posture of neutrality, MIT made no effort to clarify whether the conduct alleged violated its Rules of Use.

11.B Unauthorized Access

The superseding indictment abandoned the theory of "exceeding authorized access," and counts 9 and 12 (applicable to MIT) relied instead on "unauthorized access." The allegations in the indictment focus on numerous means whereby Aaron Swartz obtained access to the computer through unauthorized means, such as repeatedly taking steps to change his computer's apparent identities and to conceal his computer's real identity. Clearly, these are means whereby Aaron Swartz obtained access to the computer in order to engage in unauthorized conduct, that is, to do something that MIT did not want him to do through its network: engage in massive downloading of JSTOR articles.

The question posed by this charge in the indictment is, however, different: it is whether—given MIT's guest policy—Aaron Swartz accessed the MIT network without authorization. Put differently, it is whether Aaron Swartz was authorized to access the network, regardless of whether he used improper means to do so. To illustrate this distinction, the Review Panel has asked itself the following question: had Swartz, intending to engage in the conduct for which he was indicted, walked into an MIT library, shown his personal identification to the desk, and asked to log on to the MIT system as a guest—would he then have been given access? If the answer to this question is "yes," then it seems possible that Aaron Swartz's access to the MIT network was authorized, notwithstanding his inappropriate means of implementing access, or of then abusing such access (which may themselves have been violations of different criminal or civil prohibitions).

The Cambridge Detective involved in the prosecution explained to the Review panel that he repeatedly asked, in various ways, whether the laptop was authorized to be in closet; whether the cable from the laptop to the network switch was authorized to be there; whether the manner of downloading the articles was authorized; and, overall, whether the method of accessing and using MIT's network in this manner was authorized. He was told "no," and told that MIT had tried to prevent the downloading by disconnecting the computer of the (then) unknown suspect.

The Review Panel questioned five employees of MIT's IS&T who were involved in the identification and monitoring of Aaron Swartz's laptop found in the network closet of Building 16 and who provided information to the prosecution during its preparation of the criminal case. According to them, and also according to OGC and MIT's outside counsel, at no time, either before or after the arrest of Aaron Swartz, did anyone from the

prosecution inquire as to whether Aaron Swartz had authorized access to the MIT network.[3] Given MIT's open guest policy, it might be argued that Aaron Swartz accessed the MIT network *with* authorization.[4] Put differently, there is apparently an issue as to whether Aaron Swartz was authorized to access the network, regardless of the considerations that (1) he might have used improper means to implement such access; and (2) once he was on the network, he might have used such access for an improper purpose.

The relevance of this distinction can be seen in the Department of Justice's computer crime manual, Prosecuting Computer Crime (2nd ed.)[5], published by the Office of Legal Education, Executive Office for United States Attorneys:

> A more difficult question is whether a person with some authorization to access a computer can ever act "without authorization" with respect to that computer. The case law on this issue is muddy, but, as discussed below, there is growing consensus that such "insiders" cannot act "without authorization" unless and until their authorization to access the computer is rescinded.[6]

As far as the Review Panel could determine, MIT was never asked by either the prosecution or the defense whether Aaron Swartz's access to the MIT network was authorized or unauthorized—nor did MIT ask this of itself.[7] Given that (1) MIT was the

---

[3] The Cambridge Detective also told the Review Panel that, in the later stages of the prosecution, he asked IS&T personnel whether Aaron Swartz was authorized to access the network and was told that he did not. None of the IS&T personnel questioned by the prosecution recall such a question being asked, and the Review Panel has found no indication that the Secret Service Agent or the federal prosecutors made such an inquiry.

[4] *See Wentworth-Douglass Hosp. v. Young & Novis Prof'l Ass'n*, No. 10-cv-120-SM, 2012 U.S.Dist. LEXIS 90446 (D.N.H. June 29, 2012) (distinguishing between a violation of a computer use policy and a violation of computer access restrictions).

[5] http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

[6] There is also complexity and ambiguity in the definition of exceeding authorized access. The manual states:

The CFAA defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."

…

Accordingly, to prove that someone has "exceeded authorized access," prosecutors should be prepared to present evidence showing (a) how the person's authority to obtain or alter information on the computer was limited, rather than absolute, and (b) how the person exceeded those limitations in obtaining or altering information.

[7] The Review Panel asked the following question of five IS&T employees who were involved in the events around discovery of the laptop: "Was Aaron Swartz authorized to access the MIT network?" It received the following answers:

(1) Probably yes.

(2) After MIT began trying to disconnect the laptop from the MIT network, no.

alleged victim of counts 9 and 12, (2) the MIT access policy, its Rules of Use, and its own interpretation of those Rules of Use (including the significance or "materiality" of any violation of those terms) were at the heart of the government's CFAA allegations in counts in both indictments, and (3) this policy and these rules were written, interpreted, and applied by MIT for MIT's own mission and goals—not those of the Government—the Review Panel wonders why.

11.C Losses Exceeding Five Thousand Dollars

The indictments alleged that MIT suffered more than $5,000 in losses due to Aaron Swartz's conduct. Under the CFAA, the term "loss" is defined[8] as:

> [A]ny reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

The only "loss" as defined above—here being "out of pocket costs" incurred by MIT resulting from Swartz's conduct—was the cost of copying documents and the cost of the surveillance camera placed in the basement closet of the Dorrance Building on January 4, 2011. These totaled less than $5,000.[9] All other expenses were attributable to salaried personnel who would have been paid their full salary whether these events had or had not occurred. Thus, from MIT's perspective, the Review Panel does not find that MIT suffered losses relevant for CFAA exceeding $5,000 resulting from the conduct of Aaron Swartz.[10]

---

(3) His means of access was not authorized, but he, personally, was authorized as a guest.
(4) It is unclear.
(5) There is no black and white or yes or no answer. Since 1987, the MIT policies regarding its network have been implemented with the intent to educate and guide, never to litigate. As a guest, he had authorization to access the MIT network, but he was not authorized to get on the system the way he did.

The Review panel did not request of MIT a formal answer to this question, inasmuch as the purpose of this review was not to assess the government's allegations in this case, but rather to study how MIT responded to events. Similarly, the Review Panel draws no conclusions as to whether the other counts in the indictment did or did not have merit as they might pertain to MIT, or whether Swartz's access of the JSTOR system was or was not lawful.

[8] 18 U.S.C. § 1030(e)(11).

[9] Alternatively, one might argue that the few days that JSTOR severed MIT from its service was a "loss" suffered by MIT that could be determined by prorating MIT's yearly payment of service fees to JSTOR. However, to the knowledge of the Review Panel, this calculation was never made or sought.

[10] The Review Panel's finding would be different if MIT had hired outside personnel to conduct the necessary investigation, or had paid its own personnel overtime to do so. *See Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands Int'l Inc.*, 616 F. Supp. 2d 805, 811 (N.D. Ill. 2009) ("The CFAA states that a company that pays for damage assessment may satisfy the loss requirement."). We note that in *United*

Whether or not this $5,000 jurisdictional amount was met by the actual losses incurred by MIT appears to be relevant to only count 4 of the initial indictment and count 13 of the superseding indictment, pertaining to damages caused by intentional or reckless conduct. The remaining counts brought under the CFAA (counts 2 and 3 and counts 3 through 12, of the initial and superseding indictments respectively) include for their jurisdictional amounts the value sought or obtained by the conduct, and not merely the actual loss caused by the conduct. Thus the number and value of the JSTOR articles downloaded by Aaron Swartz would be included when calculating the jurisdictional amount for these other counts.

States v. Middleton, 231 F.3d 1207 (9th Cir. 2000), the Court found that where a computer had been damaged and its problems needed to be fixed, it was appropriate to use the prorated time spent by employees to fix those problems as the value of the damage. Here, however, no damage was caused to the MIT computer, no problems were fixed, and the Review Panel concludes that *Middleton* is not applicable.

Appendix 12: LETTER FROM JSTOR TO ITS PUBLISHERS

This is the full text of the June 10, 2011, letter from JSTOR to its publishers, as discussed in report section III.A.4.

Dear Colleagues–

I am writing to make you aware that JSTOR experienced a significant misuse of its database in which a substantial portion of the content was downloaded in an unauthorized fashion using the network at one of our participating universities. The situation has been remedied and the data are secure, though I wanted to alert you given the scale of the incident and to share additional steps we are taking to prevent these occurrences in the future.

The content that was taken was systematically downloaded using an approach designed to avoid detection by our monitoring systems. Fortunately, we were able to uncover the activity and worked with the institution to isolate the source on campus and to stop it. An individual believed to be responsible for this activity was later identified. We understand this person was not affiliated with the school.

Our highest priority has been to secure the content and ensure that it not be distributed. I am pleased to report that the data have been turned over and we have received a signed agreement from the individual identified in which this person confirmed that the downloaded content has not and will not be used, copied, transferred, or disseminated.

We have also undertaken a review of our monitoring systems to guard against future efforts of this kind. Stroz Friedberg, a firm specializing in this area, has been retained to help us enhance the security of our systems as well as our monitoring techniques. Additionally, we have contracted with Attributor, experts in antipiracy solutions used by many publishers, to monitor the Internet for content that might have been inappropriately downloaded from JSTOR.

This is a matter that we take very seriously. Over the years, JSTOR has had practices in place to monitor for excessive usage as well as to locate and remove copies of materials online that people may have inadvertently or inappropriately taken from JSTOR and subsequently posted elsewhere. We will continue to develop and improve our systems to be responsible stewards of your content.

I invite you to call or email me with any questions you may have about this situation.

Sincerely,

Laura Brown
EVP and JSTOR Managing Director

Appendix 13: LEGAL PROCEDURE AND PRACTICE IN CRIMINAL INVESTIGATIONS AND PROSECUTIONS

The investigation and prosecution of Aaron Swartz was in many ways a straightforward matter, and in other ways very complex. However, both categories of the relevant activity are outside the experience of most laypersons, as well as that of many attorneys who do not practice criminal law or who are not familiar with the laws governing computer crime and electronic communications.

13.A The U.S. Department of Justice and the United States Attorneys

The United States Department of Justice (DOJ) is the primary law enforcement agency of the United States, although its role inside the federal government is not limited to the handling of criminal matters. A more thorough understanding of the DOJ and its multiple functions may be found on its website: http://www.usdoj.gov.

The head of the Department of Justice is the Attorney General, who is a cabinet-level official, appointed by the President and confirmed by the U.S. Senate. Under him are a Deputy Attorney General and an Associate Attorney General, and various Assistant Attorneys General (AAGs), all of whom are similarly appointed by the President and confirmed by the Senate.

The DOJ is divided into numerous divisions including, for example, the Criminal, Civil, Civil Rights, and Environmental Crimes Divisions, each of which is headed by an Assistant Attorney General. The DOJ also includes multiple agencies that have their own administrative structures. Among those agencies are the Federal Bureau of Investigation (FBI), the Marshals Service, and the U.S. Bureau of Prisons.[1] To various extents these agencies and their heads report to the Attorney General and those under him.

Federal prosecutors fall into two categories: (1) Trial Attorneys and their supervisors, these being the Assistant Attorneys General and their deputies; and (2) United States Attorneys and their assistants, called Assistant U.S. Attorneys (AUSAs).

Trial attorneys are employed as part of the government's civil service, and are primarily stationed within Washington, D.C. They are assigned to various divisions within the DOJ that have responsibility for prosecuting federal crimes, such as (but not limited to) the Criminal Division. The Criminal Division itself is divided into various sections and units, each of which has a particular area of expertise. One of these is the Computer and Intellectual Property Section.

---

[1] The Secret Service reports to the Department of Homeland Security.

The United States Attorneys are appointed by the President and confirmed by the Senate.[2] Their terms are for four years. Each is assigned responsibility for one of the 94 judicial districts into which the United States is divided, although one United States Attorney has responsibility for two districts, those of Guam and the Northern Mariana Islands. Thus, there are 93 United States Attorneys. The authority of a United States Attorney does not extend outside of his or her district.

Under the U.S. Attorney for each district are a number of Assistant United States Attorneys, known as AUSAs. They are not civil servants, but are appointed by the Attorney General upon the recommendation of the U.S. Attorney for a district.

To a significant extent, the U.S. Attorneys and their AUSAs function autonomously from the DOJ. The interaction between the U.S. Attorneys' Offices and the DOJ is complex. For example, for most matters, Trial Attorneys from DOJ must be invited by the U.S. Attorney in order to prosecute or assist in the prosecution of a crime in his district, otherwise they will not be allowed by the district court to participate in the court proceedings. Also, the use of some criminal statutes to prosecute a defendant, such as the Racketeer Influenced and Corrupt Organizations (RICO) Act, and the use of some prosecution and investigative techniques, such as grants of immunity or wiretaps, by a U.S. Attorney or AUSA must be approved by the appropriate Assistant Attorney General or Division within the DOJ. However, as a general matter, the following can be said: U.S. Attorneys and their AUSAs have primary responsibility for enforcing the federal criminal statutes within their districts, and do so without direct supervision or permission from the Attorney General or the DOJ.

Because the DOJ has responsibility for the entire United States, it sees similar types of criminal cases on a more regular basis than does a typical U.S. Attorney's Office. That is one of the reasons why its divisions are themselves divided into sections and units: each of these smaller subdivisions has an expertise in a particular area of the law. In addition to being available to prosecute cases across the country that are within their particular specialties, the attorneys within these subdivisions are available for consultation with AUSAs in the various districts.

13.B The Investigative Agencies

Although the DOJ and some U.S. Attorneys' Offices have their own investigators and auditors who assist prosecutors in preparing and pursuing a case, the investigation of a criminal matter is usually done by a specific agency having independent law enforcement

[2] In addition to a presidential appointment, an interim U.S. Attorney may be appointed by the Attorney General. 28 U.S.C. § 546.

authority. Some of these are administratively within the DOJ, such as the FBI, the Drug Enforcement Administration, and the Marshals Service. Others are outside of the DOJ, and are within other departments of the executive branch of the government. One such example is the U.S. Secret Service, which is administratively part of the United States Department of Homeland Security. Others are the various Offices of the Inspector General (OIG) of various departments and agencies, such as the OIG for the Department of Health and Human Services. Under all of these scenarios, the investigators within these law enforcement agencies do not report to and are not supervised by the prosecutors with whom they work when a case is under investigation or prosecution.

Federal law enforcement investigators are referred to as "agents," and most agents are categorized and referred to as "special agents." Among other powers, special agents are authorized to carry and use firearms.

13.C The Federal Criminal Investigation: Pre-indictment

Criminal investigations conducted by the federal government are opened, and may be conducted separately, by a prosecutor and by a law enforcement agency. Typically, a law enforcement agency, such as the Secret Service, will start an investigation and may proceed with it for a significant time before deciding that it wishes to pursue a prosecution. At that point, the agent handling it (or, less often, his supervisor) will meet with a prosecutor, such as an AUSA, and ask that his office also open a criminal investigation. At this stage, such open investigations are referred to as "matters." How such matters are opened, and who is assigned to a matter once opened, varies from office to office among the U.S. Attorneys' Offices. Several additional points are worth noting.

A prospective defendant does not have to be identified at the time that an investigation or criminal matter is opened. Similarly, it is not necessary to establish that, in fact, a crime has occurred in order for a criminal matter to be opened. It is not uncommon for a matter, once opened, to be closed when it becomes apparent, for example, that no crime has occurred; that the perpetrator of a crime cannot be found or is outside the reach of the law; that the proof necessary to obtain a conviction is not available; or that a particular criminal incident is not worth the time and resources needed to successfully prosecute the perpetrator.

The arrest of a person who is under investigation is normally accomplished after the issuance of a warrant by a federal judge. The application for a warrant is called a "complaint," which describes the evidence known to the prosecution that justifies issuance of the warrant. A complaint charges a person with having committed a specified crime. The burden that must be carried by the prosecution, when seeking an arrest warrant on a complaint, is that the evidence show "probable cause" that a crime was committed and that the named defendant committed the crime. Exculpatory evidence or

possible defenses do not have to be included in the complaint. Alternatively, a law enforcement agent can arrest someone without a warrant if he or she directly observes a suspect commit a serious crime, usually a felony. In the federal system, once such an arrest is made, the suspect is promptly brought before a federal judge, where the agent explains the evidence that provoked the arrest. This is done under oath. The judge then decides whether probable cause existed to justify the arrest, and, if such a ruling is made, the suspect—now the "defendant"—is held in custody pending a determination of any terms for his release on bail.

For serious crimes, *i.e.*, felonies, a defendant has the right to be charged by way of grand jury indictment before being subject to trial, conviction, and punishment.[3]

A grand jury is composed of 23 persons, and conducts its proceedings in secret. The grand jurors are selected from a panel of potential jurors, much as is a trial jury. However, for the grand jury, the selection process occurs in closed session with a judge and a prosecutor, and no defense attorney is present (as there is no defendant or potential defendant at this point). Grand juries usually sit for a period of 18 months, and consider a wide-ranging and continually changing collection of criminal investigations, although it is not uncommon for a grand jury to focus upon just one, complex investigation. In such instances, the court may extend a grand jury's term beyond 18 months if the grand jury is investigating a complex matter and cannot complete the investigation without the extension.

Quorum for a grand jury is 16 persons, and it takes 12 persons to approve or return an indictment. The votes occur in secret, with no one present but the grand jurors. The foreman of the grand jury is one of their members whom they have voted to serve in that role. It is this foreman who will sign all of the indictments approved by the grand jury, and who will return and "hand up" the indictments to the judge when approved.

A grand jury has enormous leeway for conducting investigations. It is free to engage in "fishing expeditions," and it can compel witnesses to appear to testify and can compel the production of documents. The Assistant U.S. Attorney serves as counsel to the grand jury, giving it legal advice, guiding its investigations, issuing its subpoenas for witnesses and documents, and doing most of the questioning of the witnesses who appear. It is the Assistant U.S. Attorney who drafts the proposed indictments presented for the grand jury's consideration (although in theory the grand jury can propose and draft its indictments, as well as issue its own subpoenas and call its own witnesses). All of the grand jury's proceedings are secret, to protect the grand jurors from outside influence and

[3] The Fifth Amendment to the Constitution provides that "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia when in actual service in time of War or public danger."

to prevent potential defendants from learning what the grand jury is investigating and what the prosecutors may have learned about their activities. Although it is rare that a grand jury refuses to approve a proposed indictment presented to it by an AUSA, such refusals do occur, and the resulting declination is known as a "No Bill."

Once an indictment has been voted on and approved, it is handed up to a judge (sitting "above," on a bench) by the foreman in what is a straightforward session, usually with a prosecutor accompanying the foreman. At that time the indictment, with the names of the defendants and the facts alleged that set forth the crimes with which they are charged, becomes a public document. Occasionally, the prosecutor may ask the judge receiving the indictment to seal it, that is, to keep out of the public's view. This is usually done in one of two situations: where there is concern that the defendants will flee upon learning that they have been charged with criminal offenses before they can be taken into custody; and where the grand jury is continuing its investigation and the prosecutor does not want the returned indictment to "tip off" those still under investigation about what the grand jury is investigating and what it knows.

The burden that must be met before an indictment may be returned is that 12 grand jurors must find that "probable cause" existed to conclude that the proposed defendant committed the crime or crimes to be charged. Put simply, probable cause means that the facts asserted are probably true, and that a crime was probably committed by the defendant. Once such a finding has been made, a warrant for the arrest of the defendant may issue from the court.

13.D The Arrest

As already discussed, an arrest can take place upon a warrant issued upon an indictment or a complaint, or if a law enforcement officer observes the defendant committing the crime charged.

Once arrested, the defendant must be brought promptly before a judge. This is known as the "initial appearance." If no warrant had been issued, the judge will hold a hearing to decide whether or not the arrest is justified. Also, bail may be set, and counsel may be appointed (if the defendant is indigent and cannot afford to retain counsel from his own resources). If no indictment is returned within 20 days of an arrest (with or without a warrant), an additional proceeding, known as a "preliminary hearing," may be held, where the government will be put to its proof—that is, the prosecution will have to introduce evidence before the court, subject to cross examination and rebuttal by the defendant, demonstrating that probable cause exists that the defendant committed the crime charged. If the court concludes that the government has not carried its burden, then the charges must be dismissed and the defendant is released from custody or from the terms and conditions of his bond. However, such a dismissal is usually without prejudice,

meaning that the prosecution is able to "try again" after it accumulates more evidence. Generally, prosecutors try to avoid preliminary hearings, which can serve as early discovery opportunities for defendants to learn the strengths and weaknesses in the government's case, and try to obtain an indictment either before an arrest is made or within the 20-day window before the preliminary hearing must be held.

At some point, an arraignment will take place. An arraignment is where the defendant is advised by the court of the charges in the indictment and their penalties (sometimes the court requires the defendant's attorney to do this), and the defendant is asked to enter his plea: guilty or not guilty.[4]

At some point, sometimes at the arraignment, and sometimes at a status conference held afterwards, a plan for scheduling and determining the scope of discovery is agreed upon by the parties or ordered by the court. Sometimes the terms of this discovery plan are largely predetermined by the rules of the local court. Discovery in criminal cases is very different than that used in civil cases. The prosecution and the defense each have advantages and disadvantages relative to the opposing party.

13.E Investigations, Discovery, and the Asymmetric Nature of Criminal Litigation

Criminal litigation is very adversarial. It is also very asymmetric. The prosecution has the advantages of: the use of the grand jury to investigate the case before indictment; one or more federal agents to continue the investigation pending trial; the use of search warrants; and powers to compel testimony from reluctant witnesses through grants of immunity obtained from a court. On the other hand, the defense can raise the shield of the Fifth Amendment privilege against self-incrimination, to avoid disclosing information known to the defendant, and perhaps only to the defendant; and it can force the government to prove the defendant's guilt—beyond a reasonable doubt and to the unanimous satisfaction of 12 *petit* jurors—without having to put on a shred of evidence or cross examine a single government witness. The burden to convict rests solely with the prosecution, and the defense need do nothing if it so wishes.

The prosecution's investigation typically begins with a grand jury. As stated above, a grand jury can, if it so wishes, go on a "fishing expedition." It can issue subpoenas for the production of documents from third parties and the testimony of witnesses.

A grand jury subpoena can be very broad (although courts will often modify or entirely "quash" such a subpoena if it appears unduly or unnecessarily burdensome to a third

[4] Other types of pleas exist, such as *nolo contendere*, which means the defendant does not admit guilt but will not contest the government's case and the court's sentence. Such additional pleas are rarely entered and almost never at arraignment.

party). The scope and timing of production by the party receiving the subpoena is often the subject of negotiation between the producing party and the grand jury's counsel, that is, the AUSA. However, the length of time that a subpoena is valid is subject to two constraints. The first is the term limit of the grand jury itself. Once a grand jury expires (say at the end of its normal 18-month term), the validity of the subpoena itself expires whether or not the grand jury's investigation was completed.

The second constraint is a bit more complex. The purpose of a grand jury is to investigate the possible commission of a crime and decide whether or not to return an indictment naming the perpetrators of that crime. Once it has done that, its job is done: a prosecutor is not permitted to use the subpoena power of a grand jury in order to continue to investigate a case for the purpose of amassing additional evidence for use at trial. However, a grand jury is allowed to continue to investigate a matter if it is exploring additional charges other than the ones it initially returned, or wishes to consider indicting additional defendants. Also, sometimes a second grand jury may revisit an indictment returned by a previous grand jury, for the same purposes, or to correct a mistake made in the initial indictment. Under these circumstances, the second grand jury may conduct its own investigations and issue its own subpoenas to accomplish these purposes.

Once the indictment has been returned, the defendant has been arrested and arraigned, and the court's discovery plan has been entered, true discovery begins. Instead of broad, grand jury subpoenas available only to the prosecution, both sides now have the use of much more limited trial subpoenas available under Rule 17(c) of the Federal Rules of Criminal Procedure. They are colloquially known as "17(c) subpoenas." These subpoenas may be served on any third parties who have evidence relevant to the issues to be argued at trial, but are subject to the following limitations: (1) they are limited to demanding the production only of documents calculated to produce evidence relevant for trial (rather than to investigate the case); and (2) absent a court order to the contrary, the deadline for compliance with their terms is the date of trial or a specific pretrial hearing. Thus, the defense, which never had the advantage of the broader grand jury subpoenas, is limited in what it can obtain, and as to the timing of when it can obtain it.

Criminal discovery between the parties, that is, the information that one side must turn over to the other, is governed primarily by Rule 16 of the Rules of Criminal Procedure and by several important Supreme Court rulings. In a very broad-brush summary:

1. The prosecution must produce to the defense any exculpatory information that it might possess, that is, anything that might show that the defendant did not commit the crimes charged (this is known as *Brady* material, after the Supreme Court case announcing this rule).

2. The prosecution must also produce any information that might be used to impeach government witnesses, that is, information that might cast doubt on the veracity of the government's witnesses, such as prior crimes of dishonesty, plea deals or immunity agreements with the government, etc. (this is known as *Giglio* material, after the Supreme Court case that announced this rule).

3. The prosecution must surrender any statements of the defendant that it might seek to introduce at trial, recorded or otherwise.

4. The prosecution must identify any expert witnesses that it might introduce.

Also, at the request of the defense, the prosecution must turn over the exhibits that it intends to introduce at trial; however, if it does this, then the defense is obligated to do the same.

The defendant has a Fifth Amendment privilege against self-incrimination: he does not have to tell the government anything, and for the same reason the ability of the government to compel him to produce documents and tangible items is limited. Also, he has the right to force the government to prove his guilt without having to disprove anything in the government's case. For this reason, the rules governing discovery are weighted in the defendant's favor: he can choose to give the government nothing, but will still be entitled to obtain items as listed above.

13.F Interviews and Compliance with Subpoenas

The defense is severely limited in that it cannot compel a third-party witness to talk to it prior to trial, to learn what he or she might say, in contrast to the prosecution, which had the opportunity to seek such a witness's testimony during a grand jury proceeding.

Third parties must comply with subpoenas (grand jury or otherwise), and must be truthful during any testimony they give or interviews with government investigators to which they consent—if they mislead the government, they can themselves be subject to prosecution for perjury, the making of false statements, or obstruction of justice. However, absent a subpoena or a court order, a third-party witness is not obligated to tell or give the prosecution or the defense anything, no matter how important might be what he knows or the evidence that he has.[5]

[5] A caveat is 18 U.S.C. § 4, which makes it a felony to knowingly fail to disclose actual knowledge of a felony offense; however, the Supreme Court has added the requirement that to violate this statute, one must engage in some additional conduct serving to cover up the offense.

13.G Pretrial Motions and Hearings

The parties have the opportunity to file motions in order to limit the issues that will be presented at trial. This is usually done by the defense in an effort to narrow the charges brought, and the evidence introduced against the defendant by the prosecution. Two of these motions are the motion to dismiss and the motion to suppress.

A motion to dismiss is what its name implies: a request by the defense to the court asking that an indictment, a count in the indictment, or a particular legal theory within a particular count be removed from the jury's consideration. Depending upon when the motion is filed and ruled upon, an advantageous ruling—a dismissal—may be with or without prejudice. That is, the prosecution may or may not be able to seek an amendment to its indictment[6] and correct the flaw identified by the defense and adopted by the court. The primary issue will be whether the ruling comes down before or after the trial jury that is to hear the case is sworn.

The Fifth Amendment of the Constitution prohibits any defendant from being "subject for the same offense to be twice put in jeopardy of life or limb." The manner in which this prohibition is applied is that, once a trial jury is sworn, the government cannot appeal or seek a superseding indictment if a charge is dismissed by the court. Thus, if a dismissal is ordered by the court before the jury is sworn, the government has the opportunity to "try again." If it is ordered after the jury is sworn, the defendant is forever acquitted of that charge.

A motion to dismiss is usually brought on the grounds that, even if the facts alleged in a count are correct, those facts do not set forth a violation of the law that is charged. Thus, it may be argued—as it was in the *LaMacchia* case discussed in Appendix 9—that even if the defendant, David LaMacchia, did what the government alleged he did, what he did was not a crime.

Closely allied with this concept is the criminal doctrine of "lenity." This doctrine applies to the language used in a criminal statute and to the extent to which such language is ambiguous. Put simply, if a statute can be read in two different ways, one exonerating the

[6] An "amended" indictment is referred to as a "superseding indictment."

defendant, and the other convicting him, the benefit of the doubt must be given to the defendant and he must be acquitted of the charge. This doctrine arises from the Due Process Clause of the Fifth Amendment, which provides that no person "shall be deprived of life, liberty, or property without due process of law . . . ." A pedestrian definition of "due process" is this: notice and an opportunity to be heard. "Notice" means adequate notice, such that a reasonable person can understand the conduct that the statute proscribes. Thus, if a criminal statute is so ambiguous as to be read in two contradictory ways, one of which exonerated a defendant charged with its violation, then it is the more lenient of the two readings which the courts will apply to the considerations of the defendant's guilt or innocence.

A motion to suppress is different in that it does not directly attack a charge brought by the prosecution, but instead attacks the evidence the prosecution intends to introduce in order to prove that the defendant committed the crime as charged. For example, if a police officer entered a person's home without a warrant and without any judicially acknowledged exception to the requirement for a warrant, and he found and seized contraband such as drugs, counterfeit currency, or bombs, that contraband would, on a motion to suppress, be held to be excluded from introduction, and from the consideration of the jury, at trial. Put simply, evidence illegally found and seized is not admissible against a defendant whose rights have been violated by the illegal search and seizure.

A motion to suppress, if successful, is a very powerful blow against the prosecution, given the heavy burden it bears of having to prove guilt in a case "beyond a reasonable doubt." Often, after a motion to suppress is granted, the prosecution will choose to forego pursuing a trial rather than expend its resources in an attempt to obtain a conviction in much weakened circumstances.

13.H The Status of "Victims" in Federal Prosecutions

The federal Crime Victims' Rights Act was enacted in 2004. It provides for a number of procedural rights that must be accorded to victims of a crime that is the subject of a criminal prosecution. These are:

1. The right to protection from the accused
2. The right to notification
3. The right not to be excluded from proceedings
4. The right to speak at criminal justice proceedings
5. The right to consult with the prosecuting attorney
6. The right to restitution

7. The right to a proceeding free from unreasonable delay
8. The right to be treated with fairness, and respect for the victims' dignity and privacy

In the federal system of criminal justice, a victim of a crime does not have the right to "press charges," that is, to authorize the prosecuting officials to pursue criminal charges against a suspected perpetrator; nor does he or she have the right to refuse officials permission to pursue such charges. The power and discretion as to whether or not to prosecute a person who is suspected of committing a crime is vested entirely with Department of Justice, subject only to the limiting powers of the grand jury and the courts.

Appendix 14: QUESTIONS FROM THE MIT COMMUNITY

At the outset of this review, the Review Panel set up a website where MIT community members could post questions about the Swartz incident. This appendix lists the questions, together with our answers.

1. What support, if any, does MIT offer for students undergoing federal investigations or criminal charges? If none, why not?

Answer: MIT students facing criminal investigation or prosecution have several MIT resources available to them for guidance and support, including Student Support Services and, if needed, MIT Medical. The Office of the General Counsel cannot provide legal advice or representation to students—nor to faculty or other members of the MIT community—on their personal legal issues. Professional responsibilities governing lawyers prohibit the OGC from representing individuals in their personal issues because the OGC represents only MIT. The OGC refers individuals needing personal advice to sources of legal assistance, and when asked, OGC will provide general guidance and assistance to community members as to finding counsel.

2. It appears that Swartz was not intending to sell any JSTOR content. Does this mean the main charge was trespassing?

Answer: The initial indictment by a federal grand jury on July 14, 2011, charged Aaron Swartz on four felony counts: one count of wire fraud and three counts of violating the Computer Fraud and Abuse Act (CFAA). A superseding indictment was returned by a second grand jury on September 12, 2012, and charged Aaron Swartz with 13 felony counts, these being two counts of wire fraud and 11 counts of violating the CFAA. The CFAA can be violated regardless of whether the accused individual makes any commercial use of content obtained. For a full description of the charges please see the Report, section II.B.1 *The state prosecution*, and section II.B.2 *The federal prosecution*.

3. Is the MIT Office of Legal [sic] Counsel comfortable supporting MIT hacker culture, even (or especially) in legal gray areas?

Answer: This is an issue for serious discussion by the MIT community as a whole, not only the Office of the General Counsel. Please see the Report, Part V, *Questions for the MIT Community*, Question 7.

4. Why did MIT continue to support the charges against Aaron after JSTOR dropped their case?

Answer: MIT took no position on the criminal charges against Aaron Swartz, either before or after the JSTOR settlement. The report section III.A.4 *MIT discusses possible public statements with JSTOR* addresses in detail the history of MIT's interaction with JSTOR about possible statements, in anticipation of the indictment in July 2011. After the indictment, MIT did not issue any statements. It did not support the charges, nor did it advocate that they be dropped. Report section IV.B *Neutrality: Issuing Statements; Providing Information to Prosecution and Defense* discusses some of the options MIT had here.

5. Why is it that you [MIT] get to review yourself?

Answer: MIT typically assigns the responsibility of internal reviews to members of its community who were not directly involved with the events under review and who MIT believes will make a thorough and impartial review. The Review Panel for the Aaron Swartz matter also included one individual who has no MIT affiliation.

6. Doesn't MIT have the right to monitor (including w/ video) its own property, and hand that evidence over to the police if it feels there is a trespasser?

Answer: MIT has the right to use video to monitor its own property. Regarding the handing over of evidence, please see the Report, section I.B *Discovery of the Laptop*; section IV.A.3 *Providing information to law enforcement pre-subpoena*; and Appendix 10 *Legal Analysis of MIT's Provision of Documents and Packet Capture*.

7. What options did MIT have in terms of issuing a public statement in support of Swartz? At what points would it have been legally possible to issue a statement? Possible under MIT policy? Was this option considered at these junctures?

Answer: Making a public statement was indeed an option considered by MIT at various stages of the events related to Aaron's prosecution. It would have been legally possible to do so at any time, and no formal MIT policy would have prevented it. Please see the Report, Part III *MIT's Response to the Prosecution*; and section IV.B *Neutrality: Issuing Statements; Providing Information to Prosecution and Defense.*

8. Is there any record of Aaron attempting more straightforward/cooperative ways of downloading articles?

Answer: The report notes two of Aaron Swartz's previous experiences with downloading large numbers of articles, both of which appear to have been done in a straightforward

manner. (See the Report, section II.A.2 *Possible motives for downloading.*) We have no evidence that he attempted to download the JSTOR files at MIT in a more straightforward or cooperative way, nor of his seeking permission from JSTOR for research on its database through his Harvard appointment, which provided access to JSTOR through Harvard's network.

9. Does MIT believe that copying the wrong bits warrants prison time?

Answer: MIT as an institution has been a leader in promoting open access and strongly supports fair use for academic and research purposes. While there are a lot of different opinions about copyright law within the MIT community, the general stance of MIT towards open access is something to be explored. Please see the Report, Part V *Questions for the MIT Community*, Question 6.

10. What is the record of prosecutor Carmen Ortiz arranging any plea bargain, either favorable or draconian, weeks before a trial?

Answer: The Review Panel's charge was to review the actions of MIT's offices and individuals, not those of the U.S. Attorney, so we did not explore the record of U.S. Attorney Ortiz or the Boston Office, beyond the Aaron Swartz case.

11. What MIT officials are in charge of protecting privacy of electronic records (logs)?

Answer: The Office of the General Counsel with Information Services and Technology together determine the Institute's policy on the privacy of electronic records. The Report suggests that these policies be reviewed. See Part V *Questions for the MIT Community*, Question 2.

12. Were MIT's data retention and collection policies appropriate here? You cannot disseminate what you do not have.

Answer: Please see the Report, Appendix 7 *Records Produced by MIT to Law Enforcement*; and Part V *Questions for the MIT Community*, Question 2, which suggests a review of MIT's electronic record collection and retention policies.

13. What are MIT's policies on investigating and prosecuting abuse of network resources? Were those policies followed in this case? Are those policies appropriate to our institutional culture?

Answer: MIT's first response to abuse of network resources is to contact the Stopit Group. Please see the Report, section I.A *Downloading of JSTOR Articles* for a description of MIT's response to the Swartz downloading; and the questions for the MIT

community raised in Part V of the Report, which address some of the issues related to network resources and the MIT culture.

14. Were MIT's actions in this case consistent with MIT policy and with actions taken in prior situations when an individual was caught "misusing" the MIT network and network resources? If not, then why?

Answer: MIT's actions in the Swartz matter appear consistent with actions taken by the Institute in prior situations, although the initial response was to a situation that was unique in the magnitude of the downloading and the fact that the owner of the laptop was unknown. Please see the Report, section I.A *Downloading of JSTOR Articles*. For MIT's actions after that, and the considerations of whether they were consistent (or should be), see Part V *Questions for the MIT Community*, Questions 1 and 5; and Appendix 9 *Some Prior Relevant Incidents at MIT*.

15. Given MIT's tradition of student "hacks," MIT officials should ask: How would we have responded if Aaron Swartz had been an MIT student and had performed his actions by hacking into Harvard's network? And how would we have wanted Harvard to respond?

Answer: These are important questions for the MIT community to address. For a discussion of these issues, please see the Report, Part V *Questions for the MIT Community*, Question 7.

16. So why was he arrested, after all?

Answer: The initial state charge at the time of Aaron Swartz's arrest was breaking and entering. For the federal indictment, he was accused of violating the Computer Fraud and Abuse Act and committing wire fraud. For a full description of the charges, please see the Report, section II.B.1 *The state prosecution*; and section II.B.2 *The federal prosecution*.

17. What view did MIT take of the "superseding indictment" (additional charges) against Swartz and did it play a role in influencing (or trying to influence) the indictment one way or another? Who from MIT testified at the grand jury and what did they say?

Answer: MIT had no advance knowledge of the superseding indictment and played no role in influencing the indictment either before or after it was issued. No one from MIT testified at the grand jury for the second indictment.

18. Who told MIT Police to say Swartz had "no known address"?

Answer: The report in part describes the actions of the MIT Police in the course of the downloading investigation and the arrest of Aaron Swartz. Aaron Swartz refused to speak to the police at the time of his arrest. The Incident Report completed by the MIT Police after the arrest indicts that his residence was "IL," that is, Illinois. The Review Panel speculates that the arresting officers saw Mr. Swartz's driver's license or other identification card from his hometown, in Illinois, and, not knowing his Massachusetts address, simply listed "IL" for Mr. Swartz's residence.

19. What can MIT do to hasten reform of the academic publishing industry?

Answer: MIT has an ongoing interest in promoting open access of scholarly publications. For details of this activity and ideas for doing more, please see the Report, Part V *Questions for the MIT Community*, Question 6; and Appendix 8 *MIT and Open Access Publishing*.

20. At one point did the secret service become involved in this investigation?

Answer: The Secret Service became involved when MIT asked the Cambridge Police for assistance when the laptop was found on campus in a restricted network closet, automatically downloading JSTOR articles. A special agent of the U.S. Secret Service accompanied the Cambridge Police detective who came to the MIT campus in response to the call for assistance. Please see the Report, section I.B *Discovery of the Laptop*.

21. To what extent did the larger context influence MIT's actions in this matter, particularly MIT's evident willingness to throw students to the dogs, even before all of the facts are in?

Answer: A small number of past incidents involving MIT students who became involved in legal disputes are discussed in the Report, Appendix 9 *Some Prior Relevant Incidents at MIT*. Also, section III.A.3 *MIT adopts and maintains a posture of neutrality* describes the extent to which the experience with one of these prior incidents may have influenced MIT's actions on the Aaron Swartz matter. See also Part V *Questions for the MIT Community*, especially Questions 1, 7, and 8.

22. Harvard's general counsel (Bob Iuliano) told a [Harvard] Law School professor not to advise Swartz. What did he tell MIT to do?

Answer: The Review Panel has no knowledge of Harvard's General Counsel providing any advice to MIT (or to Harvard professors).

23. Reaching out to the family?

Answer: The Review Panel communicated with Aaron Swartz's father several times, and met with him twice. The Panel also spoke and met with Taren Stinebrickner-Kauffman, Aaron Swartz's partner. The MIT Media Lab hosted a memorial for Aaron Swartz, and the Review Panel arranged a brief impromptu meeting for Robert Swartz with MIT's President. We are unaware of any other attempts by the administration to reach out to the family.

24. Did MIT contact the Justice Dept. on the JSTOR case or did the Justice Dept. contact MIT? Was MIT aware then or at any time that Swartz was being [sic: had been] investigated by the US gov't. on matters other than the JSTOR business?

Answer: The U.S. Attorney's Office chose to become involved in response to reports from a Secret Service agent accompanying the Cambridge Police detective who came to the MIT campus in response to the call to the Cambridge Police for assistance when the unidentified laptop was found in a network closet. Please see the Report, section I.B *Discovery of the Laptop*. MIT had no awareness of any of Aaron Swartz's past activities (including his having been investigated by the FBI) until a few days after the arrest. And the only matter the Review Panel is aware of that involved a government investigation of Aaron Swartz occurred in 2008, when Mr. Swartz downloaded about 20 million pages of documents from the government-run PACER (Public Access to Court Electronic Records) system. For details of this incident, please see the Report, section II.A.2 *Possible motives for downloading*.

25. What, if anything, did MIT learn from its involvement in the federal prosecution of its student David LaMacchia back in 1994?

Answer: As far as the Review Panel could determine, the MIT personnel and officers who handled the Swartz matter did not relate this to the LaMacchia case. Please see the Report, Part V *Questions for the MIT Community*, Question 1; and Appendix 9 *Some Prior Relevant Incidents at MIT*.

26. Is this the best an MIT 6.3 [Electrical Engineering and Computer Science] Professor can do to create and facilitate a discussion about MIT policy and its relationship to the Justice system? Or is this a way to make it as difficult as possible to post and discuss these issues?

Answer: This website was designed for posting questions, not for hosting discussions. Discussions of the issues in this Review are important, and we recommend that the MIT administration create an appropriate forum for that.

27. Is MIT's reaction in the Swartz case symptomatic of a longer-term cultural drift?

Answer: The report raises this issue for discussion in Part V *Questions for the MIT Community*, especially Question 8.

28. Which powerful parties have an interest in this report being written a certain way, perhaps to cover up wrongdoing or protect MIT's reputation? How were they allowed to directly or indirectly influence the report?

Answer: The Review Panel has tried to write a thorough report, based on an accurate representation of the facts as we determined them, and free of bias and of influence from any individuals or groups regardless of whether they were connected to the events being investigated. See Appendix 4 on the processes that the Review Panel followed.

29. Who within MIT was not forthcoming in providing information that could have been helpful to this report?

Answer: The Review Panel believes that it received complete and accurate information from all parties, both within and outside MIT, who were asked to provide information that contributed to the content of the report.

30. In general, how long does MIT keep logs? Does it need to keep them for that long? Are there processes in place such that formulated log policies will always be as minimal as possible?

Answer: Because there are many different types of computer and network logs, it is difficult to provide a general answer regarding MIT's retention policies and practices in this area. For a discussion of these issues, please see the Report, Part V *Questions for the MIT Community*, Question 2; and Appendix 7 *Records Produced by MIT to Law Enforcement*.

31. What role did JSTOR play in the prosecution? What interaction occurred between JSTOR and MIT, and is there any historical precedent for such interaction?

Answer: JSTOR settled potential civil claims that it could have brought against Aaron Swartz. His defense counsel used this settlement agreement in an effort to convince the U.S. Attorney's Office to forgo a prosecution or drop the demand for jail time. For a description of this, please see the Report, section II.C *Aaron Swartz's Settlement with JSTOR*. For a description of interactions between JSTOR and MIT prior to Aaron Swartz's arrest, please see the Report, Part I *Events Leading to the Arrest*; for interactions after the arrest, please see section III.A.4 *MIT discusses possible public statements with JSTOR*. The Review Panel is not aware of any historical precedent for these interactions.

32. Should MIT policies favor freedom of Information vs. the right of authors to a fair compensation?

Answer: MIT has an active interest in open access to scholarly publications. For a discussion of MIT's activities in this area, please see the Report, Part V *Questions for the MIT Community*, Question 6.

33. Were MIT faculty/staff even informed of the Swartz break-in incidents?

Answer: Staff in the MIT Libraries and in Information Services and Technology knew of the downloading of JSTOR articles when it was discovered in September 2010. MIT's Director of Libraries briefed the Academic Council on these incidents shortly afterwards.

34. What were the reasons to hand over network usage data without a subpoena?

Answer: MIT provided logs and captured packets to the federal law enforcement officers when they requested it. MIT judged that in this situation it was appropriate to provide that information without a subpoena. Please see the Report, section I.B *Discovery of the Laptop*; and Appendix 7 *Records Produced by MIT to Law Enforcement*.

35. What influence, if any, did MIT exercise or could it have exercised in the plea negotiations? Did MIT really scuttle a plea bargain with no prison time?

Answer: MIT played no role in any plea negotiations related to the Aaron Swartz case. For a description of these negotiations, please see the Report, section II.B.2 *The federal prosecution*. For a description of MIT's position regarding the government's prosecution, please see Part III *MIT's Response to the Prosecution*. It is unclear whether MIT could have exercised influence on the plea bargain. Please see in particular section III.A.2 *MIT is informed about the prosecution*; and section III.C.3 *MIT's outside counsel speaks with the lead prosecutor*.

36. Did anyone at MIT involved with any matter involving Aaron Swartz, violate an MIT policy in ignorance?

Answer: The Review Panel did identify areas of policy that might be reviewed and clarified going forward. For example, MIT's provision of records as described in the report reveals some gaps in its policies and practices around electronic records. Records were given to the Secret Service and the USAO with the approval of OGC, but there seems to have been lack of clarity between OGC and IS&T over exactly what had been approved, and how long that approval lasted. Some records were turned over prior to subpoenas being issued. Some records were retained longer than MIT's retention policy called for, and for some of kinds of records there seems to be no explicit retention policy

at all. For a discussion of these issues, please see the Report, Part IV *Decision Points for MIT* and Part V *Questions for the MIT Community*.

37. Did anyone at MIT put an obligation or consideration outside MIT policies, ahead of MIT policies?

Answer: The Review Panel did not find instances where anyone at MIT acted outside the boundaries of specific policies but it did identify areas of policy that might be reviewed and clarified going forward. Please see the Report, Part IV *Decision Points for MIT* and Part V *Questions for the MIT Community*.

38. Did anyone at MIT have to choose between conflicting MIT policies in dealing with Aaron Swartz's actions and their aftermath? What were those policies? How can these conflicts be resolved?

Answer: The report provides discussion on MIT policies related to the Aaron Swartz matter that might benefit from review and clarification going forward. Please see the Report, Part IV *Decision Points for MIT* and Part V *Questions for the MIT Community*.

39. At what point, and why, was the US Secret Service called in to investigate?

Answer: The Secret Service became involved when MIT asked the Cambridge Police for assistance when the laptop was found on campus in a restricted network closet, automatically downloading JSTOR articles. A Secret Service agent accompanied the Cambridge Police detective who came to the MIT campus in response to the call for assistance. Please see the Report, section I.B *Discovery of the Laptop*.

40. Why did MIT personnel hand over data about Aaron (including DHCP logs and other intercepted network information) to the Secret Service, without a warrant, court order, or subpoena?

Answer: MIT believed it was appropriate to provide information without a subpoena to law enforcement officers about the network usage of the unidentified laptop that was found in a network closet. It did so in view of the fact that law enforcement was conducting an investigation into what was potentially ongoing criminal activity of unknown scope.

For a description of these events, please see the Report, section I.B *Discovery of the Laptop*; and Appendix 7 *Records Produced by MIT to Law Enforcement*. For a discussion of the issues related to providing such information, please see section IV.A.3 *Providing information to law enforcement pre-subpoena*; Part V *Questions for the MIT Community*, Questions 1 and 2; and Appendix 10 *Legal Analysis of MIT's Provision of Documents and Packet Capture*.

41. Why did MIT hand over evidence to the government? Why didn't MIT just shut down the computer and instead set up a video camera? Were these actions illegal, under wiretapping laws?

Answer: MIT provided information to law enforcement officers both before and after being issued subpoenas for information. MIT also set up a video camera to help identify the operator of the laptop. MIT judged these actions to be legal, and the Review Panel concurs. For a description of these events, please see the Report, section I.B Discovery of the Laptop. For a discussion of the legal issues related to providing such information, please see section IV.A.3 *Providing information to law enforcement pre-subpoena*; Part V *Questions for the MIT Community*, Questions 1 and 2; and Appendix 10 *Legal Analysis of MIT's Provision of Documents and Packet Capture*.

42. It would have been clear to anyone following the case that the government was treating Swartz unfairly. Why didn't MIT issue a public statement saying that they did not support the government charges against Swartz?

Answer: MIT decided against issuing a public statement of any kind with regard to the government's charges against Aaron Swartz. For a detailed discussion of MIT's position in this matter, please see the Report, Part III *MIT's Response to the Prosecution*; and Part V *Questions for the MIT Community*, Question 8.

43. Swartz's family has alleged in the press that MIT promised not to release more data to law enforcement than it had to, and not to do so without a warrant. Yet it seems to have done so. How can this be?

Answer: We are not aware of this claimed allegation from Aaron Swartz's family, but in any case MIT made no such promise. MIT did tell the family that it had not turned over any information without a court order. This claim was mistaken. In any case, MIT provided information to law enforcement officers both before and after being issued subpoenas for information. See the Report, section I.B *Discovery of the Laptop*; and section IV.A.3 *Providing information to law enforcement pre-subpoena*.

44. Assuming that everyone did their jobs correctly, what were the point(s) at which MIT staff could have known or SHOULD HAVE KNOWN that Swartz would be faced with federal charges with penalties of decades in jail? Who had the option to stop this?

Answer: The federal investigation was opened on January 5, 2011, before the arrest, and MIT learned of the investigation at the time of the arrest. In March 2011, the lead prosecutor informed MIT that the prosecution was going forward. (See report section III.A.2 *MIT is informed about the prosecution*.) MIT first learned of the actual federal

charges against Aaron Swartz, and the possible penalty, only when this information was first made public in the indictment in July 2011. MIT judged that it did not have the option to stop the prosecution. For perspective on this judgment, see report section III.C.3 *MIT's outside counsel speaks with the lead prosecutor*. For a discussion of MIT's position in this matter, see the Report, Part III *MIT's Response to the Prosecution*.

45. Why isn't students' work free/open by default?

Answer: According to MIT Policies and Procedures, students generally own their own work. So it's up to students whether to make their work free/open. The exception is that MIT owns the work if it was developed under sponsored research funds or if it makes significant use of MIT resources. For more information, see MIT Policies and Procedures[1] section 13.1, and the MIT Technology Office's Guide to the Ownership, Distribution and Commercial Development of MIT Technology.[2]

46. I'm an alum. I'm withholding contributions until this is adequately addressed. Anyone with me?

Answer: As the Review Panel, we've presented the facts as well as we could, and we've raised issues to help MIT learn from this experience. The next steps are up to the entire MIT community—alumni included.

---

[1] <http://web.mit.edu/policies/13/13.1.html>
[2] <http://web.mit.edu/tlo/www/community/policies.html>

Appendix 15: GLOSSARY

The following is a list of words used in the report that the lay reader to a particular discipline (e.g., computer science, law, etc.) may wish to refer to in order to more completely understand the language of the report[1]:

Accelerator Company: A business entity that, in return for a partial ownership interest in a new company, provides investment and other assistance to the startup company's founders to assist rapid growth.

Access Controls: Restrictions placed on the access to a place or resource. As used in this report, they are computer software or hardware that limits access to a network, computer, or computer resource to a particular user, or to a particular form, or in some other manner.

Address or Addresses: An "address" is a number assigned, or a numerical label given, to a device connected to a computer network. Such devices include computer workstations, laptops, printers, scanners, *etc*. An address is used both to identify the particular interface on the device (MAC "Media Access Control" address), and to specify where on the network the device is connected (IP "Internet Protocol" address).

Aggregator: A computer program, a computer application, or an entity that collects and organizes a specific type of information from multiple sources, and provides the results to third parties, often for a fee.

Aided and Abetted: A legal term that means a person either assisted in or facilitated a criminal act, or was himself assisted or otherwise aided in the performance of a criminal act. Under federal criminal law, a person who "aids, abets, counsels, commands, induces or procures" the commission of a criminal act is punishable as if he or she performed such act himself or herself. See 18 U.S.C. § 2.

Archival Back Runs: Prior issues of a publication going back in time from the current issue.

Arraignment: A court proceeding at which a defendant is informed of the criminal charges against him and offers his plea of guilty or not guilty. This is not the same as an initial appearance, held immediately after an arrest, where bail may be determined but no plea is required.

---

[1] Some of the definitions contained in this Glossary are based in part on explanations found in Wikipedia.

Arrest: The taking into custody of a person, under lawful authority.

Assistant U.S. Attorney: An attorney who, working under the authority of a United States Attorney, represents the United States of America in criminal or civil cases in which the United States of America is a party. The term is frequency abbreviated as "AUSA." An AUSA is appointed, by the Attorney General of the United States, to serve in a particular judicial district and under the direction of a particular U.S. Attorney. As part of their responsibilities, AUSAs serve as counsel to the grand juries seeking and considering evidence that may lead to an indictment of a criminal defendant.

Attorney-Client Privilege: A legal doctrine, recognized by the courts, that protects communications between a person and his or her attorney pertaining to communications intended to be confidential and made for the purpose of seeking or transmitting legal advice. It applies in both the criminal and civil settings, and there need not be the threat of litigation for it to be applicable. The attorney-client privilege as to particular communications survives the death of a client.

Attorneys' Fees and Costs: The collective sum of monies paid by a party to its attorneys in a legal proceeding, for both the fees charged by the attorneys and for the expenses incurred by the attorneys. It does not include expenses incurred by the party.

Backup: In the context of this report, the term "backup" means the provision, or appearance, of one or more additional law enforcement personnel at the scene of an incident to provide support to officers already present.

Blog: A discussion site on the World Wide Web, comprised of distinct posts. The word "blog" is a contraction of the words "web" and "log."

Boot Camp: As used in this report, a business boot camp is a workshop focused on giving an individual with an entrepreneurial idea a set of skills and information that will help the individual more rapidly and successfully convert the idea into an active business.

Byte: A unit of data, consisting of 8 bits, where each bit is either 0 or 1.

Cambridge District Court: The District Court located in Cambridge. District Courts are Massachusetts Trial Courts that have limited jurisdiction. They preside over criminal matters with a potential sentence of up to five years imprisonment and civil matters in which the damages sought do not exceed $25,000, and other miscellaneous matters.

Capture: As used in the context of computer communications, the term "capture" means to make a copy of electronic data being transferred between and among computers and networks.

Captured Packets: Data packets that have been received or recorded after or during transmission. See **Data Packets**.

Certified Copy: A copy of a document attested to by the holder or issuer of the original as being identical to the original.

Civil Action: A civil lawsuit. That is, legal proceedings initiated by one party, the plaintiff, claiming that another party, the defendant, has violated the law in a manner that causes the defendant to be liable for injuries suffered by the plaintiff.

Civil Liability: An obligation imposed by law to pay money, whether in the form of compensation, punitive damages, or fees and costs, to a party, arising from injuries suffered by that party.

Class A Network: Devices located on the Internet are allocated IP addresses, which are in the form of a sequence of four separate numbers (each ranging from 0 to 255) separated by dots, *i.e*., 12.234.056.11, or generally, www.xxx.yyy.zzz.[2] These numbers form a hierarchy, similar to a residential address being described by state, city, street name, and street number. For IP addresses, the highest level in the hierarchy, *i.e*., the state, is identified by a number that is referred to as the "Class A." This is the first of the four numbers in the sequence. As one gets closer to the location of the actual device, one moves lower in the hierarchy, to the second number (Class B), then to the third (Class C), and finally to the device itself (the last number). Since the numbers used to denote the higher levels in the hierarchy can be viewed as groups of addresses located on networks and subnetworks, the classes are themselves referred to as networks, *e.g*., the Class A network, the Class B network, and the Class C network.

Class C Network: See **Class A Network**.

Computer Crime and Forensics: Computer crime is criminal activity committed by means of computers, networks, or the Internet. Computer forensics is the detection and investigation of potential computer crimes, or the use of computers in criminal activity, where such investigation is conducted for the purpose of obtaining information in a manner suitable for use in a court of law.

Computer Fraud and Abuse Act: Known as "CFAA," a wide-ranging criminal statute that prohibits a person from engaging in various activities involving computers or networks. It has both criminal and civil penalties, including forfeiture provisions, and its violation may result in either felony or misdemeanor punishments. See 18 U.S.C. § 1030. It

[2] This description is for Internet Protocol version 4 (IPv4), which is what the MIT network used in 2010 and uses today.

focuses, among other matters, on "protected computers," which is defined as including any computer or computing device that affects interstate or foreign commerce; thus, any computer used to connect to or communicate on the Internet qualifies as a protected computer. Among its various criminal provisions are gaining unauthorized access to a computer, and exceeding authorized access. Determining whether or not an individual has violated these provisions often requires the interpretation of the Terms of Services of the owner or operator of a computer, system, or network, and the materiality of various terms. The Act also contains provisions prohibiting the fraudulent use of a computer, and recklessly causing damage to a computer.

Conspiracy: In the criminal context, an express or tacit agreement by two or more individuals to act in concert to commit a crime.

Content Downloading: The act of accessing a device or website and requesting it to transmit files so that they can be viewed or stored, where the files may be articles, videos, photographs, programs, data, etc.

Cookie: A file or segment of code placed or stored on a user's web browser. While the user browses the Internet, websites will add or modify such files to add or monitor information placed on the user's computer. Such information may include prior visits to various websites, and may be used to track a user's browsing history. It may also be referred to as an HTTP cookie, a web cookie, or a browser cookie.

Copyright: A legal doctrine granting the creator of an original, creative work certain exclusive rights in the use and publication of the work. In the United States, the power to specify and grant this right is assigned by the Constitution to Congress, and the laws that have been enacted concerning copyrights provide both civil and criminal prohibitions against their infringement. Copyrights automatically apply once an applicable work is created. The United States Copyright Office, a part of the Library of Congress, maintains a registry of copyrights that creators may use to document their ownership of a work.

Copyright Infringement: Interference with the rights of a copyright holder, such as by making or distributing copies of a copyrighted work, or making changes to a copyrighted work, without the permission of the copyright holder.

Count: The compilation of the specific language in a civil complaint or criminal indictment alleging that one or more defendants violated a particular legal prohibition. In the criminal context, a count is the charging language in an indictment alleging that one or more defendants violated a specific criminal statute. Each count must identify the criminal statute by citation, and must allege sufficient facts so as to put each defendant on notice as to (1) the specific conduct in which the government accuses them of having

engaged and (2) the basis on which the government asserts that such conduct is a violation of the statute cited.

Crash: A situation in which a computer device or software program ceases to function properly.

Creative Commons: This is a nonprofit organization devoted to expanding the range of creative works available for others to legally share, use, and improve upon. It was founded in 2001 by Lawrence Lessig of Harvard University, Hal Abelson of MIT, and Eric Eldred of Eldritch Press with support of the Center for the Public Domain. The organization has released several free copyright licenses to the public. They allow the creators of works to specify which rights they reserve, and which rights they waive for the benefit of the general public.

Cryptography: A method or technique of hiding communications from third parties. In the field of computing, it is the electronic encoding of communications, requiring a predetermined procedure or key in order to convert the encoded communication into a readable or otherwise understandable format.

Damages: The sum of monies claimed by a plaintiff as legal compensation for injury or other loss suffered by the plaintiff.

Data Packet: Information is transmitted on computer networks as sequences of separate units called "data packets." These are reassembled upon reaching their destination.

Data Stream: Data packets while in transmission on a network or between computing devices.

Demand for Discovery: The making of a formal request for discovery from an opposing party or a third person. See **Discovery**.

Deputized: An appointment as a substitute with the power to act on behalf of the person who made the appointment. As used in this report, the MIT Campus Police officers were deputized to act with the power of Middlesex County Police officers near the MIT Campus.

DHCP: Dynamic Host Configuration Protocol is a protocol used on a network to assign IP addresses to devices so that they can communicate through the network.

DHCP Client ID: An address or identification label assigned to a device by the **DHCP Server**.

DHCP Server: A device used to implement the Dynamic Host Configuration Protocol on a particular network.

DHCP Server Logs: Listings of requests from computers for the DHCP server to assign IP addresses. These records contain MAC addresses, IP addresses, and the date and time that the computers acknowledge the receipt of addresses.

Digital Information: Information represented by strings of bits, that is, zeros and ones.

Digital Content: Text, articles, photographs, video, sound, and other media maintained in a digital format.

Digital Library: An information retrieval system where collections are stored in digital formats and available for downloading via computers and networks.

Digital Millennium Copyright Act: Known as the "DMCA," a federal law with both civil and criminal penalties that prohibits the production and distribution of devices and software intended to circumvent measures used to prevent copying or other infringement of copyrighted works. 17 U.S.C. § 1201 *et seq*.

Digitized: Converted into a digital format.

Discipline: As used in this report, a field of academic study.

Discovery: In a lawsuit, information obtained by a party through formal means specified in court rules, or from another person for use as evidence at trial or to continue to investigate the issues in the case. In civil cases, such information may include answers to written questions, testimony obtained in a deposition, production of documents and other things, and admissions made in response to particular requests. In criminal cases, such information is usually, but not always, limited to production of documents.

Disk Activity: The writing of digital information to, or the reading of such information from, a hard drive by a computing device. See **Hard Drive**.

Dismissed: In the context of a court proceeding, being terminated without further hearing.

District Attorney: A public official who has responsibility for representing counties within the Commonwealth of Massachusetts in civil and criminal cases. The District Attorney's Office consists of the District Attorney; prosecutors and other attorneys who work under the authority and supervision of the District Attorney, formally known as Assistant District Attorneys; and support personnel. There are 11 districts established by law in Massachusetts.

Downloading: The act of accessing a device or website and requesting it to transmit data so that it can be viewed or stored.

Electronic Communication: Information composed of electronic signals, often but not necessarily in a digital format, intended to be a communication between parties.

Electronic Message: See **Electronic Communication**.

Electronic Records: A digital form of data files, readily able to be stored on a computer and accessed through a network.

Excessive Use Incident: An incident where a user significantly exceeds the use or requests for use of resources made available to or anticipated being sought by users on a network.

Expert Witness: A witness who offers testimony in the form of an opinion based on his or her having specialized knowledge applicable to an issue in a case; this is in contrast to a fact witness, who offers testimony based on personal knowledge as to facts at issue in a case. Expert witnesses are usually paid for their time learning about the case, drafting a written report about their opinions, and giving a deposition (i.e., providing a sworn statement) or testifying at trial.

External Hard Drive: A **Hard Drive** connected to a device in a manner that is external to the device.

Felony: A serious criminal offense, for which the penalty for conviction is more than one year of imprisonment and the forfeiture of some civil rights.

File Transfer Protocol: A protocol used on the Internet for the transfer of files from a source computer to a requesting computer.

Foreman: The member of a grand jury who presides over, speaks for, and signs for the grand jury, usually appointed by election of the grand jury.

Fraud: A doctrine of common law whereby one person induces a second to do something, or refrain from doing something, as a result of false, misleading, or deceptive statements, representations, promises, or conduct. The goal of fraudulent conduct is usually to obtain something of value, or to prevent the defrauded party from obtaining something of value. See also **Wire Fraud Act**.

Free and Open Source Software Movement: A movement launched in 1983 within the computer professional community, the goal of which is to establish the right of all users to freely use, study, modify, and redistribute software.

Free Culture Group: An MIT student group that promotes freedom on the Internet and in the digital world. According to the MIT website, its projects educate the MIT community "and sometimes the world" about fair use, free software, and open access.

GB: An abbreviation for gigabyte. See **Gigabyte**.

General Counsel: An attorney who functions as an entity's legal advisor and representative attorney and provides general legal advice to the entity. Usually the term refers to an attorney who is an employee of the entity, and this person is referred to as "inside counsel." Such inside counsel may have one or more assistants who are also attorneys. Sometimes, the functions of a general counsel are provided by outside, retained attorneys.

Gigabyte: A unit of measurement for an amount of electronic data. A byte is a unit of data, consisting of 8 bits, where each bit is either 0 or 1. The term "giga," when used as a prefix, means 10 to the ninth power. Thus, the term "gigabyte" means 1,000,000,000 bytes.

Grand Jury: An official body empaneled by a court to hear evidence of possible crimes and empowered to vote on and return indictments regarding such crimes and naming persons as defendants. The grand jury is composed of citizens who meet in secret at periodic, regularly scheduled sessions, usually over the course of 18 months, and who hear multiple matters concerning different investigations and potential defendants. In the federal system, a grand jury is composed of 23 people; a quorum consists of 16 individuals; and an indictment may be returned only upon the affirmative vote of 12 individuals. A person who is facing federal felony charges has a right for those charges to be considered by a grand jury, as opposed to solely by a prosecutor, and can be brought to trial only upon the vote and return of an indictment by a grand jury identifying the criminal charges he or she may face at trial. A grand jury may return an indictment upon a finding that probable cause exists that the person committed the offense under consideration.

Grand Jury Subpoena: A subpoena issued by a grand jury. It may call for the production of documents or other tangible evidence, or for testimony under oath of a person called before it. Such a subpoena has the force of an order from the court, and a failure to comply with it—absent court consent—can subject the recipient to an order of contempt, which may include jail time.

Guest Account: As used in this report, a courtesy account provided by MIT Libraries to persons who wish to use MIT's network and the resources available on that network but are not MIT students, faculty, or staff.

Hack: In the field of computing professionals, initially a term applied to a particularly creative, clever, or resourceful creation or use of programming or hardware. Also used by the general public to refer to accessing a computer system by circumventing its security structure.

Hacker: Someone who hacks. In the computer subculture, a hacker is "a person who enjoys exploring the details of programmable systems and stretching their capabilities."[3] Also used by the general public to refer to someone who exploits weaknesses in computer security.

Handed Down: In the context of a criminal proceeding, delivered by the court, such as an order or opinion being "handed down" from the bench after a ruling on a disputed issue. Contrast with **Handed Up**.

Handed Up: In the context of a court proceeding, delivered to the court, such as an indictment being "handed up" to the bench after being approved by the grand jury. Contrast with **Handed Down**.

Hard Drive: A data storage device used for storing and retrieving digital information, using one or more rapidly rotating rigid discs or platters coated with a magnetic material that retains the data even when the device is turned off. Also known as a "Hard Disk Drive" or an "HDD."

Hardware Probe: A physical device used to connect to an electronic device to test or otherwise investigate the content, functioning, operation, or design of such device.

Hexadecimal: As used in the computing fields, a base sixteen number, or a numbering system where each digit has a value from zero to fifteen. Characters and instructions used in computer languages are often written in codes based on such a format.

HTML: Hypertext Markup Language is the primary computer language used for the creation of web pages and other formats that can be displayed in a web browser.

Indictment: In the criminal justice system, a formal written accusation returned by a grand jury charging a defendant with having committed one or more specified crimes. In the federal system, a person who is accused of committing a felony has a right to require the government to obtain an indictment in order to maintain the prosecution and obtain a conviction. The burden carried by the government when seeking an indictment from a grand jury is to establish probable cause to the satisfaction of at least 12 grand jurors (out of a possible 23), in contrast to the burden at a criminal trial, which is proof beyond a reasonable doubt established to the unanimous satisfaction of 12 *petit* jurors. The right to indictment by a grand jury during a felony prosecution is found in the Fifth Amendment of the U.S. Constitution. Misdemeanors may be prosecuted without the return of an indictment, and upon the filing with the court of an "information," which is an alternative charging document drafted and signed by a prosecutor.

---

[3] See <http://en.wikipedia.org/wiki/Hacker_(programmer_subculture)>.

Initial Appearance: In the federal criminal system, the first appearance of a criminal defendant before a court after the defendant has been formally arrested or charged with a crime though a criminal complaint or, in some cases, citation. At this hearing, bail may be set. Contrast with **Arraignment**. In some state systems, an examination of the evidence may also occur to determine whether there is sufficient evidence to permit the prosecution to go forward.

Internet Archive: A nonprofit digital library providing permanent storage of digitized information, and free access to the public of such material. The materials include websites, video, and books.

Internet Protocol: A protocol whereby servers and other devices on the Internet communicate and transmit data and requests for services; and whereby networks comprising the Internet do the same.

IP Address: "Internet Protocol Address," which is a number that identifies and locates a device on the Internet. See **Address**.

IP Address Range: A range or group of IP addresses. See **IP Address**. The term is usually used in the context of a group of IP addresses that may be available for a particular use, or within which a particular device may be found.

IS&T: MIT's Information Services and Technology, the organization within MIT responsible for computer network maintenance and security.

Latent Fingerprint: A fingerprint of a person, normally not visible to the naked eye, left on the surface of an object that has been handled by that person. A latent fingerprint is the result of perspiration or other materials that emanate from the skin's surface ridges. These are detected and made visible by dusting or another process, at which point they can be compared to known fingerprints on file.

LED: Light emitting diode, a semiconductor source of light.

License: A legal grant, by a person who controls the rights over something, that permits the receiver to use or gain access to that item under circumstances where the receiver's use or access would otherwise be unlawful.

Log: A listing or catalogue of metadata maintained by a computer or network server. A typical log might identify a history of the devices a particular computer connected to; when that computer was active on a network; and the source and volume of data downloaded to the computer.

MAC Address: Media Access Control address, which is a unique identifier assigned to devices that can connect to a network. MAC addresses are usually assigned by the device manufacturer, but may be changed by a user.

Magistrate Judge: In the federal judicial system, a judicial officer of a district court, whose authority comes from statute and not the Constitution. In criminal matters, magistrate judges often hear and decide preliminary issues, such as bail or discovery disputes, but cannot make final or conclusive rulings directly addressing the guilt or innocence of a defendant. Upon the request of a district judge, however, a magistrate judge may issue a report and recommendation on such issues, which the district judge is then free to adopt, reject, or amend as he or she decides is appropriate.

Metadata: As used in this report, information about data, specifically, information about data that was transmitted, stored, or used, without identifying the data itself. Examples might be the dates and times on which electronic transmissions occurred; the size of or number of bytes in those transmissions; the IP addresses to and from which the transmissions occurred; and the MAC address of the origin or recipient of the transmissions. However, the content of the actual transmission is not included.

Misdemeanor: A criminal offense, considered less serious than a felony. The penalty for conviction thereof is one year of imprisonment or less.

MIT Police: The Massachusetts Institute of Technology's Police Department, which consists of a chief and a varying number of police officers. These are deputized by the Sheriff of Middlesex County to act as law enforcement officers within the area of the MIT campus. The MIT Police consists of a Patrol Division, within which there is the Crime Prevention Unit; and a Special Services Division, within which is an Investigations Unit.

MIT Libraries: The library system of the Massachusetts Institute of Technology, which includes the libraries of the five academic schools comprising the Institute, and their holdings, which include over three million printed volumes, over 55,000 databases and electronic journals, and a number of digital collections that increases yearly.

Monitoring: In the context of this report, the term "monitoring" means the real-time observation of a data stream across a network.

Motion to Dismiss: In the criminal justice system, a motion made by a party to dismiss one or more counts in an indictment, asking the court to find that, as a matter of law, the pertinent counts do not allege a violation of a criminal statute, or that the defendant is not liable for any such violation for other reasons. Such a dismissal, if granted by the court, may be with or without prejudice; that is, the prosecution may (i.e., without prejudice) or

may not (i.e., with prejudice) be allowed to correct the defect alleged by the motion and thus may or may not be allowed to continue the prosecution as to the affected counts.

Motion to Suppress: A formal request by a party to a judge presiding over a criminal matter to examine the means by which certain evidence in the possession of the prosecution was obtained; rule that such means was unconstitutional or otherwise unlawful; and rule that such evidence may not be introduced at trial or otherwise considered with regard to the guilt or innocence of the defendant.

Network: A "network" or a "computer network" is a system that allows computers to exchange data. The physical connection may be by cable or a wireless means, and multiple networks may themselves be interconnected.

Network Flow Data Logs: Logs created and maintained by a server located on a network comprising a history of the metadata of users on the network and the resources they requested. See **Metadata**.

Network Interface: A hardware or software system that lies between devices, or between a device and a network, and provides standardized functions that enable the devices and networks to communicate with each other.

Network Registration Database: As used in this report, a log maintained by the MIT network of the history of computers and users who have registered with MIT: the email address of the user, the date on which the user registered and signed on to use the network, whether the user was a guest, and the MAC address of the user's device.

Network Switch: A device that links segments of a network or devices on a network.

Notice of Appearance: A filing with a court made by an attorney providing notice that the attorney is now representing one of the parties in the case. The term "Entry of Appearance" is also used for the same purpose.

Office of the General Counsel: As used in this report, the term "Office of the General Counsel," or "OGC," is the internal law office of the Massachusetts Institute of Technology. It provides legal advice, counseling, and service to MIT and represents the Institute in its legal matters. Its client is the Institute, not any individual or segment of the Institute, and currently the OGC consists of the General Counsel, 11 attorneys, and support staff. The OGC may engage private law firms or attorneys—termed "outside counsel"—to advise or represent MIT in particular matters.

Open Access: The practice of allowing unrestricted access through the Internet to scholarly journals. "Unrestricted" comes in varying degrees, but the Berlin Open Access Declaration stipulates that any open access publication must give all users an irrevocable

worldwide right of access to, and a license to copy, use, distribute, transmit and display the work publicly and to make and distribute derivative works, in any digital medium and for any responsible purpose.[4]

Open Access Publishing: Publishing under **Open Access** conditions.

Open File Transfer Protocol: A **File Transfer Protocol** made available without restriction.

PACER: Public Access to Court Electronic Records, an electronic database maintained by the federal courts of the United States through which registered users may search for entries in the court's docket and filings in judicial cases as maintained by the clerks of the federal courts. Parties to a case and their attorneys may access one copy of each filing for free; otherwise, access to all filings requires the payment of a set per-page charge.

Packet Stream: A transmission of data packets. See **Data Stream**.

PDF: Portable Document Format, a file format used to represent documents in a manner independent of the hardware, software, operating system, and application used for its display.

Penetration: As used in this report, a "penetration" is an unwanted or unauthorized access to a computer or network.

Plea: A defendant's response to a criminal charge. It might be "guilty," "not guilty," or in certain courts, "no contest" (or the equivalent).

Port: As used in this report, a port is a hardware interface between a computer or a network and other computers or peripheral devices. The interface could be a physical connection or a wireless connection.

Post-Mortem: A Latin phrase for "after death," meaning the investigation and analysis of a matter after it has ended.

Private Network: A private network is a physical network connected to the Internet that uses a dedicated or private IP address range (or "address space") unavailable to outside users.

Privilege: A legal doctrine by which the courts recognize that a person may withhold information from judicial and other proceedings on the basis of some public policy recognized as having a significant societal value. Examples of judicially recognized

---

[4] Berlin Declaration on Open Access to Knowledge in the Sciences and Humanities, <http://oa.mpg.de/lang/en-uk/berlin-prozess/berliner-erklarung/>.

privileges are the attorney-client privilege, the marital privilege, and the Fifth Amendment privilege against self-incrimination.

Privileged Documents: Documents that are protected from disclosure because they contain information that is subject to a privilege, or because the act of producing them might itself constitute a statement that is privileged. An example of the latter might be where the act of producing a document would establish that the person has possession of the documents, where this might tend to show that the person obtained them in an illegal manner.

Pro Bono: A Latin phrase meaning "for the public good," commonly used by attorneys to refer to a matter in which an attorney represents a client without compensation or at a reduced fee rate because the client's matter is one that the attorney and client deem to bear on the good of the public.

Proof of Concept: A demonstration of the feasibility of a design, idea, or principle.

Proxy Server: A computer device or software application that serves as an intermediary for requests for data or services, satisfying some of those requests with limited or no forwarded access to the server to which the requests were directed.

RADIUS: Remote Authentication Dial In User Service, a service that controls access to various MIT network services, like wireless (mobile) services or printing.

RADIUS Server Logs: Logs created and maintained by the RADIUS server, which record requests by computers to use various network services. See **RADIUS**.

Recorded Streams: Data transmissions that have been copied.

Redact: The act of removing specific portions of text or other information from a document or file (often by blacking it out and so making it unreadable, while allowing the reader to recognize that the removal occurred) before the document or file is provided to readers.

Registered: With regard to MIT students, formally enrolled in a program of study.

Robotic Harvesting: The use of a software application or script to search for and extract information from websites and servers on the Internet in an automated fashion.

Root Access: Authority by a user for full access to a computer, workstation, or server on a network.

RSS: Rich Site Summary, a collection of formats used by web feeds to publish frequently updated works, such as blogs, news sites, and audio and video feeds. An RSS

"document" or page, known as a "web feed" or "feed," includes full or summarized texts, plus supporting information about publishing dates, authors, etc.

Script: A small computer program to automate and mimic tasks used with an application that would otherwise be done by a human operator.

Seal: In the judicial system, keeping a document, filing, ruling, or other thing secret from the public and sometimes from one or more parties. Enforcement of the seal is implemented through the contempt power of the court, where a judge may punish someone by incarceration or fine for breaking the seal.

Secret Keys: A series of numbers or characters composing a code or password necessary to access a device or software application.

Secret Service: The U.S. Secret Service is a federal law enforcement agency with two responsibilities mandated by law: (1) to protect national leaders, visiting heads of state and government, designated sites, and events involving national security; and (2) to safeguard the payment and financial systems of the United States. This has been historically accomplished through the enforcement of counterfeiting statutes to preserve both the integrity of U.S. currency and also coin and financial obligations. However, since 1984, the Secret Service's investigative responsibilities have expanded to include crimes that involve financial-institution fraud, computer and telecommunications fraud, false identification documents, access-device fraud, advance-fee fraud, electronic funds transfers, and money laundering as they relate to the agency's core violations.

Semantic Web: A movement led by the World Wide Web Consortium to promote standard formats for data used on the web.

Sentencing Guidelines: In the federal criminal justice system, a formal set of factors and procedures that are considered by a judge to determine the fine and period of incarceration to sentence a defendant to after a criminal conviction. These are established and contained in a publication issued by the U.S. Sentencing Commission, and they are very complex and frequently amended. Among the factors that they take into account are a defendant's criminal history, the nature of the criminal offense, the amount of harm caused by the crime, whether the defendant accepts responsibility for his conduct, whether he violated a position of trust in committing the crime, and whether he has cooperated with law enforcement in any criminal investigations. The guidelines are not binding upon the sentencing judge, but in the event that the judge does not follow them in determining a sentence, she must justify on the record her reason for not doing so.

Server: As used in this report, a device that responds to requests made across a network from other devices for specific services or data.

Shortcut URL: A shortened version of a **URL**.

Special Agent: Colloquially, the term "special agent" refers broadly to a federal law enforcement official who works in the field as opposed to solely in an office setting. Formally, special agents are criminal investigators employed by a United States government department or agency where the investigative position is classified by the U.S. Office of Personnel Management as Criminal Investigation Series, 1811, which includes FBI special agents and U.S. Secret Service special agents and others so designated. Special agents have the power to investigate potential violations of those federal laws whose enforcement is the responsibility of the law enforcement organization for which they work, and are generally armed with a gun when in the field.

Still: A static image taken from a video or movie.

Stopit Group: A group within the MIT IS&T network security team that deals with inappropriate behavior occurring on the MIT network. A typical tactic used by the groups is to send an email to the offender, asking the person to stop the conduct in question.

Student Information Processing Board: A longstanding MIT student group, known as "SIPB," that focuses on helping students access computing resources and use them effectively.

Subpoena: An order commanding a person to appear before a court or other official body to testify, or to produce specified documents or other tangible items. A subpoena is often issued upon application of an attorney, as an officer of the court, who is representing a party in a civil or criminal case. Under such conditions, an attorney many sign and serve a subpoena without prior approval by a court. Grand jury subpoenas are typically issued by an AUSA on behalf of the jury. One exception is "Rule 17(c) subpoenas," which can be issued by the prosecution or defense in a trial. They are limited to demanding the production of documents calculated to produce evidence relevant for trial (rather than to investigate the case).

Superseding Indictment: An indictment returned by a grand jury that supersedes or replaces an earlier indictment. It may be returned by the initial grand jury that produced the earlier indictment, or it may be returned by a new grand jury that has reviewed the same evidence as the initial grand jury plus new evidence. Reasons for the prosecution seeking a superseding indictment include correcting an error in the earlier indictment; adding new defendants or new charges; and expanding the scope in terms of time or range of the criminal activity relative to that charged in the initial indictment.

Supervised Release: In the federal criminal justice system, a specified period of time that begins after a convicted felon is released from imprisonment, during which the person, as

a further part of his sentence, is monitored by a probation officer for the purpose of ensuring that he complies with restrictions imposed by law on his behavior.

Surrender: To voluntarily allow a law enforcement official to take the surrendering individual into physical and legal custody. This is typically done by the surrendering individual by appearing at the law enforcement office or at a courthouse after charges have been filed.

TAG: The Technical Architecture Group of the World Wide Web Consortium (W3C). (See **World Wide Web Consortium**.) The W3C "created the TAG to document and build consensus around principles of web architecture and to interpret and clarify those principles when necessary."[5]

Terms & Conditions of Use: As used with regard to the Internet or to computing services, a written set of rules to which a person wishing to use computing resources must agree in order to obtain permission to access or use those resources. It is typically in the nature of a contract or a license.

Terms of Release: Specified conditions of behavior to which a defendant must adhere during the period before trial subsequent to being charged with a crime. The setting of these conditions usually accompanies the setting of bail. They are imposed by order of the court when a defendant is allowed to remain free during this period (as opposed to being detained during the time period, which amounts to forced confinement in a detention center or equivalent).

Terms of Service: Also known as "TOS." See **Terms & Conditions of Use**.

Theory of Criminality: A theory or basis asserted by the prosecution as to why or how a defendant violated a particular criminal law. It is often apparent from the allegations of fact contained in the count of an indictment alleging the particular violation.

Tweet: A text messages of up to 140 characters broadcast by an individual using the Internet to that person's "followers" on Twitter. See **Twitter**.

Twitter: A microblogging service that allows a user with an account to broadcast text-based messages of 140 characters or less. These are known as "tweets." To receive such "tweets" of a particular user, one must register to "follow" that user. See **Tweet**.

United States Attorney: A federal official, normally appointed by the President and confirmed by the Senate, who is charged with three responsibilities: the prosecution of

---

[5] See <http://www.w3.org/2001/07/19-tag>.

criminal cases brought by the United States; the prosecution and defense of civil cases in which the United States is a party; and the collection of debts. (See 28 U.S.C. § 547.) The official title is abbreviated "U.S. Attorney." A U.S. Attorney has a staff of anywhere from several to several hundred Assistant U.S. Attorneys, who are each appointed by the Attorney General of the United States. There are 93 U.S. Attorneys. Each U. S. Attorney is appointed to be responsible for one United States federal district (with the exception of one, who is appointed to oversee two districts—those of Guam and the Northern Mariana Islands). In Massachusetts, the Office of the United States Attorney is divided into three divisions, with physical offices located, one each, in Boston, Springfield, and Worcester.

URL: Uniform Resource Locator, an address on the web where a particular web page, file, or other resource can be located. It is in the form of a character string, such as: www.mit.edu.

USB: Universal Serial Bus is an industry standard for cables, connectors, and communication protocols used by computers and electronic devices to communicate with each other.

USB Device: As used in this report, a USB device is a hardware device that can connect to a computer or other electronic device to download and store data. See **USB**.

Virtual Private Network: A Virtual Private Network, or "VPN," is based on the concept of a private network. It extends the address space, that is, the devices accessible within the private network, across the Internet (or other network) by treating outside addresses as if they are within the private network. See **Private Network**.

VPN: See **Virtual Private Network**.

Web: See **World Wide Web**.

Westlaw: A corporation that offers an extensive range of legal databases to subscribers or on a pay-for-access basis. The term is often used to refer to the service itself.

Wire Fraud Act: The Wire Fraud Act is a federal criminal statute, 18 U.S.C. § 1343, that prohibits the use of wire or wireless communications to engage in fraud. Specifically, the Act provides that:

> [W]hoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or

> sounds for the purpose of executing such scheme or artifice [has committed an offense].

The penalty for violating the Act is a fine of $250,000, or imprisonment of not more than 20 years, or both.

Wireless: As used in this report, the term "wireless" means a method whereby a device connects to a network using radio signals, with no physical connection between the device and the network.

Workstation: A high-end desktop computer designed for resource-intensive technical or scientific applications. They are commonly connected to a local area network, that is, a network of limited size and usually not integrated into the Internet. The term "workstation" also refers to a personal computer (PC) connected to a network.

Wired Network: A network whose devices are connected by cables or similar physical linking mechanisms.

Wireless Network: A network whose devices are connected by radio or other electromagnetic communications (i.e., infrared transmissions).

World Wide Web: Also known as the "web," "WWW," or "W3," a system of links that connect files and documents maintained on the Internet. The text in these documents composing the links is known as "hypertext," and a user can navigate from document to document, across servers and networks.

World Wide Web Consortium: Also known as the "W3C," the primary organization for establishing standards for the World Wide Web.