ORAL ARGUMENT HAS NOT BEEN SCHEDULED

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,

Appellee

v.

ELAINE CIONI,

Appellant

No. 09-4321

APPELLANT'S BRIEF

JENIFER WICKS

The Law Offices of Jenifer Wicks
The Webster Building
503 D Street NW Suite 250A
Washington, D.C. 20001
(202) 393-3004

Appointed by the Court for Appellant

TABLE OF CONTENTS

TABLE OF CASES, STATUTES AND OTHER AUTHORITIES

Cases

Statutes, Regulations and Misc

STATEMENT OF SUBJECT MATTER AND APPELLATE JURISDICTION

A. Statement of Basis for Subject Matter Jurisdiction in District Court.

Because Mrs. Cioni was charged with offenses against laws of the United States which allegedly occurred in the Eastern District of Virginia and his conviction was in the US District Court for the Eastern District of Virginia, the United States District Court for the Eastern District of Virginia had subject matter jurisdiction pursuant to 18 U.S.C. §§ 3231, 3237, 28 U.S.C. § 2255.

B. Statement of Basis for Jurisdiction in the Court of Appeals.

On March 6, 2009 in open court and by amended judgment on March 17, 2009, respectively, the district court issued Judgment, respectively, that disposed of all claims with respect to Mrs. Cioni. Mrs. Cioni filed a timely notice of appeal. Therefore, this Court has jurisdiction over this matter pursuant to 28 U.S.C. § 1291 and Fed.R.App.P. 4(b).

STATEMENT OF ISSUE PRESENTED FOR REVIEW

Whether the Court erred in denying pretrial motions to suppress evidence and dismiss counts and the indictment

Whether the Court erred in prohibiting cross examination under Federal Rule of Evidence 412

Whether the Court erred in denying the motion for a judgment of acquittal

Whether the Court denied Mrs. Cioni a fair and reasonable sentence where she was denied the right to counsel, Federal Rule of Criminal Procedure 32 was violated and the court failed to consider 18 U.S.C. § 3553.

STATEMENT OF THE CASE

By superseding indictment on September 11, 2008, Mrs. Cioni was charged with Conspiracy (to intentionally access protected computers without authorization and exceeding authorized access to protected computer in furtherance of intentionally gaining access without authorization and exceeding authorized access to a facility through which an electronic communication service is provided and thereby obtaining electronic communications in electronic storage in such systems), 18 U.S.C. § 371, 1030(a)(2)(C), 2701, Computer Intrusion, 18 U.S.C. § 1030 (2 counts), unlawful access to stored communications, 18 U.S.C. § 2701, and harassing telephone calls, 47 U.S.C. § 223. App. 26. After a jury trial, she was convicted on December 15, 2008. App. 107. A preserved motion for a judgment of acquittal was denied on January 9, 2009. App. 111. Mrs. Cioni was sentenced on March 6, 2009 to concurrent sentenced of 15 months on all counts of conviction (1-2, 4-6) and timely filed a notice of appeal.

STATEMENT OF THE FACTS

GOVERNMENT EVIDENCE

Meir Cohen was the president and cofounder of Teltech Systems. 12/8/2008 at 41. Teltech came into existence with the reaction of the "spoof card" which changes the phone number that would appear on a caller id for the call being made. *Id* at 41-42. Someone wanting to use the service can sign up with a credit card or paypal account at spoofcard.com . *Id* at 42. By calling the toll free access number, a user can call any number and use any number to appear as where the call is coming from; through the system, a user can disguise their voice or record the call. *Id* at 43. Teltech maintains records of activity (call logs and recordings) on a customer's account as well as billing information, payment logs and customer notes. *Id* at 43-44. Government Exhibit 1, 1-1, and 1-23 are the information subpoenaed from his company. *Id* at 45-48. He explained the various records of the business contained in those exhibits. *Id* at 48-54. What his business does is completely legal. *Id* at 54. Unless the products are used with a malicious intent, they are all legal. *Id* at 54-56. One can spoof an IP address – the address that is displayed to reflect the computer being used but it is very difficult; you can also change the identify of an IP address by proxy. *Id* at 56-57. The account was requested to be cancelled and all records deleted on October 26, 2007; this account was closed on October 30, 2007 and three calls were made after that. *Id* at 58-62.

The account records contained a message field "I requested that all records associated with my credit card be deleted. I received an email that they had been deleted. I just checked the pin and there were two calls listed. I just deleted them. Please confirm that all records associated with my credit card are irretrievable. I'm a little anxious. Even though I was just spoofing for fun, someone didn't think it was funny and lied to the police and said that the spoof caller was threatened to harm the family. Have you received a subpoena for my records? I never ever threatened anyone." *Id* at 63.

Bruce Enger lived in Chantilly, Virginia for 6 years and Tucson, Arizona for 12 years before that. *Id* at 64. He was employed as the Chief Financial Officer at Long & Foster in Chantilly, Virginia and prior to that, in Fairfax, Virginia. *Id* at 64-65. His wife's name is Maureen and he has two children Ashley and Cory. *Id* at 65. In March 2007, he had a cell phone, blackberry and home landline, all with caller id; he or a family member would answer those phones. *Id* at 65-66. His work phone would be answered by him or his assistant. *Id* at 66-67. Starting in March 2007, while away on business, at 5:30 in the morning, he received a call from a male voice telling him "we are watching you" and then there were many calls after that. *Id* at 67-68. A lot of the calls also said "we're watching you" or disclosed personal information; the caller said you need to go back to Arizona or you need to go back to where you came from. *Id* at 68-69. The caller

would say "I'm going to take all your money" or "I'm going to get your family" or "I know where your wife is". *Id* at 69. The caller id displayed various numbers for the calls as if they were originating from his own cell phone, wife's cell phone, home phone, daughter's phone, dead uncle's phone, friends, family, mom's, dad's, fax line and lots of numbers that he did not recognize. *Id* at 70. He did not know who was calling him. *Id.* Exhibit 1-8, 1-9 and 1-10 were calls made to him; 1-12, 1-13 and 1-16 were voicemail calls. *Id* at 71-74. He changed his numbers three or four times; they changed the home number and his wife and daughter changed their numbers. *Id* at 75. He told the caller to stay away from his family, his wife was in tears a number of days and they kept a lookout for Craig Scott (someone he thought was the caller), and one call referred to him being at Jackson Hole, Wyoming, where he had been around the time of the call. *Id* at 77-78. Some of the calls referred to getting a package. *Id.* Government 27 was lists that he made for the FBI related to receiving the calls. *Id* at 81-82. On August 17, at 5:18 in the afternoon, the caller said he was going to hurt him and hurt his wife. 12/9/2008 at 6-7. He received 20-25 calls at his home and a hundred or so at his office and another hundred or so on his blackberry. *Id* at 7-8. Everyone was concerned for their safety when receiving these calls. *Id* at 8-9. He also received letters that he believed were from Craig Scott and not from who the letters were addressed from. *Id* at 11-12, 15-19; Government Exhibit 20, 21, 22, 23, 34. One letter referred to

confidential information concerning an acquisition of York Simpson Underwood; unless one was in a small circle of people, the only way to know about this would be through his email communications. *Id* at 12-13. This letter said it was from "John Forsythe" from "Gain Client, Inc"; the only person he know who worked at Gain Clients was Patty Freeman who he had a personal relationship with in Tucson, Arizona. *Id* at 13-14. The letter also referred to a lady who he and his wife had hired to crew their sailboat. *Id* at 14-15. He knew Elaine Cioni; he had hired her as retirement administrator at Long and Foster from 2004 to 2005. *Id* at 20. He had a personal relationship with her after she left Long and Foster until August 2007. *Id* at 21. He identified emails he had received from Mrs Cioni during that period of time. *Id* at 22-25; Government Exhibit 26, 31, 32, 33. He communicated with Mrs. Cioni during the investigation. *Id* at 25. His last communication with her was in May 2008 when she was screaming at him about the investigation. *Id* at 25. When the investigators asked him about Mrs. Cioni, he answered their questions and didn't deny that he had a relationship with Mrs. Cioni.; if he had know she was involved, he never would have contacted law enforcement because he didn't want the personal relationship to come out. *Id* at 26-27. He had an AOL account with a password that he didn't give to anyone other than immediate family; his family has AOL and gmail accounts. *Id* at 28-31. Sharon Thorn is a friend of Mrs. Cioni's. *Id* at 33. He never authorized Mrs. Cioni

to access his AOL personal email account and she never said anything about accessing his email. *Id* at 33. In October 2006, he had strange problems with his email account and emails would show up in his read file that he had not read; Mrs. Cioni admitted a month later that she had broken into his account. *Id* at 33-34. He was convinced that Craig Scott had done all of this. *Id* at 37-38. Craig Scott had issues with Kathy Hedrick at Long and Foster and there was reference to her in the calls. *Id* at 38-39. He had a personal romantic affair with Mrs. Cioni. *Id* at 40. Before the affair started, Mrs. Cioni had told him that she was leaving her job at Long and Foster because she was attracted to him. *Id.* Mrs. Cioni was offered more money, $20,000, if she stayed at the job where her salary had been $50,000. *Id* at 41-42. When she was leaving, he gave her a cactus plant and make a comment, when she said you do know what it looks like, that it was not to scale, referring to a body part of his. *Id* at 43-44, 69. His affair with Mrs. Cioni was not his first; he had a length affair with Patty Freeman where he lead her to believe she was moving to Virginia with him. *Id* at 45. He claimed he was not trying to be in a relationship in the fall of 2006 with Mrs. Cioni. *Id* at 47-48. On November 10, 2007, he sent Mrs. Cioni an email wherein he is describing his need to talk to her because he is afraid that she's going to expose the affair. *Id* at 48. He said she would make the contact for them to get together and he would; they continued the sexual relationship through August 2007. *Id* at 56. Whatever he got in the

envelopes, he would send them to Brenda; he did not discard anything from the envelopes. *Id* at 57. Although he testified that he was frightened by the calls, he never had and never got a security system at his house. *Id* at 57-58. Mrs. Cioni told him she had gotten into his emails in the fall of 2006. *Id* at 62. In an email in December 2006, he told her that he was mad but that he forgave her. *Id* at 63; Defendant's Exhibit 25.

Maureen Enger lived in Chantilly, Virginia for six years and in Tucson, Arizona for 13 years before that. *Id* at 71. She was married to Bruce Enger and they had two children Cory and Ashley. *Id.* She had a cellular phone and a phone at home that both had caller id. *Id* at 72. In the spring or summer of 2007, she started receiving calls from a number that was her daughter's , husband's or a family member; she would answer and there was no one there or someone would hang up. *Id* at 73. The calls progressed to a garbled man's voice speaking to her. *Id* at 73. She changed her numbers several times because the calls were very annoying, unsettling and scary. *Id* at 73. She thought that a man named Craig Scott was making the calls, a disgruntled employee from Long and Foster. *Id* at 75. When she took her son out, she would watch her surroundings , trying to be more aware. *Id* at 75. She identified three calls that were calls made to her. *Id* at 76; Government Exhibit 1-4, 1-5, 1-6, 1-7. She had an AOL email account with a password that she had not given to anyone but had written down at the house. *Id* at

79. She had not authorized anyone outside her family to access her AOL account; she never had problems access her AOL account. *Id* at 79. About a year prior to her testimony, the parental controls on her son's email had been changed and she thought maybe he had done it. *Id* at 80-81. She identified emails to the team mom of her son's football team and to her daughter when she was attending school in Arizona. *Id* at 82; Government Exhibit 24-6. Sharon Weiner was a woman they hired to go sailing with them in Greece. *Id* at 83. She corresponded with her by email and Christmas cards. *Id* at 83. There was a sexual assault at her daughter's school that she left messages about for her husband. *Id.* She did not know Elaine Cioni and evidentially she did at an employee Christmas party at her house; neither of her children knew Mrs. Cioni. *Id* at 84. She never authorized Mrs. Cioni to access her AOL email account or her son's AOL email account. *Id* at 84. She and her husband used to share a computer so she might see what was on his AOL account if it was up but she did not have password access to his account. *Id* at 85.

Charles Chamberlin worked at Chattanooga State Technical Community College as the director of network and telephone systems. An Internet Protocol Address (IP Address) is an address that is used to communicate on the internet; every device has a unique IP address and that's how device's talk. *Id* at 86. The college uses the IP address range 198.146.32.1 through 198.146.47.265. *Id.* Each

users is assigned one of the addresses when they access the internet. *Id* at 87. Staff, faculty and students were assigned a user ID and password to access the college computers. *Id.* Elaine Cioni worked in the human resources department at the college for the past 3 years and was provided with an user id and password. *Id* at 88. The computers she had access to were assigned addresses within the range he mentioned. *Id* at 88. IP spoofing would be when a computer pretends to be taking the IP address that belongs to another user. *Id* at 88-89. It would be difficult but possible for someone outside of the college to spoof a college IP address. *Id* at 89. People could use other's accounts if they left them logged on when they stepped away from their computer. *Id* at 90. He does not know how common IP spoofing is. *Id* at 90.

Sharon Weiner was married and lived in St. Lazare, Quebec, Canada. *Id* at 91. She is the artistic director of the Judson Dance Center and program director for Poseidon Charters. *Id* at 92. As program director, she is in charge of provisioning boats for yachting cruises. *Id.* The Engers were clients for two weeks in June 2007 when they rented a catamaran and sailed in the Aegean Islands and Cycladic Islands in Greece. *Id* at 92-93. She corresponded before and after the cruise with the Engers by email; she had three emails account, her personal email account being with hotmail. *Id* at 93-4. She accesses her email mainly from her laptop but uses internet cafes when she is traveling. *Id* at 94. She had never been to

Tennessee and never gave the password to anyone. *Id* at 94-5. She identified several electronic mail messages between her and Bruce Enger after the cruise and indicated that she had never given the emails to anyone nor sent a copy through the postal mail. *Id* at 95-8; Government Exhibits 22, 23. In the past year, she had had problems signing into her account and she changed the password several times. *Id* at 100. Since the investigation, she stopped saying anything too personal on her email. *Id.* She didn't know Mrs. Cioni and had not authorized her to access her hotmail account. *Id* at 101. She didn't know what the source of the problem that she had getting into her account and could not precisely say when it had happened. *Id.*

Patricia Freeman lived in Tucson Arizona and worked for Long Realty Company as an executive assistant to CFO Bruce Enger for two years and six months. *Id* at 103. She had a professional and personal relationship with Mr. Enger. Starting around June 2007, she started getting unusual phone calls on her cell phone – no one there when she answered. *Id* at 104. In 2007, Mrs. Cioni called her cell phone and asked her why she was calling her cell phone and hanging up; she told Mrs. Cioni that she was not and asked her why she was calling her cell phone and hanging up. *Id* at 109. Mrs. Cioni said she was not. *Id* at 109. Then in June or July 2008, she called again and reintroduced herself in a voice mail and said there was a situation going on here that she thought she should

know about; she called several times and left several voicemail messages. *Id* at 110. The last message was that she thought there was a matter she would want to know about that involved the FBI and "you know who", which she took to mean Bruce Engler. *Id.* She thought about it for a few days and called her; Mrs. Cioni told her about the investigation by the FBI and her relationship with Bruce that was similar to Ms. Freeman's relationship with Bruce. *Id* at 111. Mrs. Cioni asked her if she could email her and indicated that she already had her email address; they emailed for a week or so but she didn't want to email anymore so she stopped. Mrs. Cioni wanted to talk more about Bruce and information about Bruce. *Id* at 111-112. She had an aol email account that she would access from home or work or from a hotel if she was traveling. *Id* at 113. She had never been to Tennessee; she gave her password to her daughter and she would leave her account open on the computer at home where her daughter or son would have access to it. *Id* at 114. In 2006 or 2007, she was booted off her account after getting a message that someone was trying to access her account from a different location; she also could not log into her account because her password was no longer valid. *Id* at 114-5. She had no reason to associate her email problems with Mrs. Cioni. *Id* at 119. She identified Government's Exhibits 20 and 21 as emails from Bruce to her and that she had not given a copy to anyone or sent a copy through U.S. mail. *Id* at 116-117. These emails were from a year before she had any problems with her

email. *Id* at 119. She also indicated that it was not her handwriting on Exhibit 21 and that she had never stayed at the J.D. Marriott on Pennsylvania Avenue. *Id* at 117-118. She never authorized Mrs. Cioni to access her email account. *Id* at 118. In her opinion, Bruce Enger was not a truthful person. *Id* at 120.

Brenda Born was a Special Agent with the FBI since October of 2005. She had computer training in computer science as well as additional training with crimes that have been committed with a computer and a Computer Analysis Response Team (CART) tech certification. *Id* at 121. She was the lead case agent. *Id* at 122. In September 2007, she received the complaint to investigate of calls being received by Bruce Enger and his family. *Id* at 122. She received the case file from Fairfax County law enforcement who had also investigated the charges. *Id* at 123. She conducted interviews and database checks. *Id* at 124. She received phone records from Arent Fox, the law form Long & Foster used, showing the calls to Bruce Enger's number. *Id* at 125. The trace on his call showed calls coming into him from Level Three Communications (Government Exhibit 28); she subpoenaed records from Level Three Communications (Government Exhibit 18). *Id* at 125-7. This information lead her to subpoenaing bandwidth.com (Government Exhibit 19) which indicated that the source of the calls from E&M Limited which offers a service called spoof card. *Id* at 127-8. Government Exhibit 29 summarized all these records that she received. *Id* at 128.

Her investigation showed that the calls being received by Mr, Enger appeared on the spoof call records in Government Exhibit 1. *Id* at 130. The spoof card account had Elaine Cioni's name and address in the records as well as an IP address at Chattanoga State Technical Community College and payment by a credit card issued to Elaine Cioni. *Id* at 131-134. She subpoenaed the information for the email accounts associated with the spoof card account and then executed a search warrant on the account providers. *Id* at 133-5, 139--141; Government Exhibits 16, 17, 17-1. The email accounts was accessed from IP addresses associated with the college and Mrs. Cioni's residences' Comcast internet account, one account being in the name of Sharon Thorn. *Id*; Government Exhibit 4. Sharon Thorn and Elaine Cioni had been best friends since childhood. *Id* at 142. She also subpoenaed information from AOL. *Id* at 142-3; Government Exhibits 2, 2-2, 2-3, 2-4. There were six sppof card account associated with Elaine Cioni or Sharon Thorn; the phone numbers on the accounts were also associated with them. *Id* at 145-8. Government Exhibit 1-4 through 1-21 were transcripts of calls saved by the spoof card company. *Id* at 149. SA Born identified the voice on the recordings as being that of Elaine Cioni. *Id* at 151. Government Exhibit 1-3 tracked the calls from the spoof call records and the identification of the numbers called. *Id* at 155. From phone numbers associated with Mrs. Cioni, there were 84 calls to Mr. Enger's office number, 14 to his work cell, 146 to his work blackberry, 24 to Mrs. Enger's

cell, 19 calls to their home in Chantilly and 2 calls to their home in Tucson, using the voice changeover technology. *Id* at 155-157; Government Exhibit 1-3. Government Exhibit 1-2 summarized the business records – summarizing the access into Mr. Enger's voice mail where the caller was able to hear unopened message or delete a message; she summarized this evidence by listening to the calls. *Id* at 159-160. Based on interviewing Sharon Thorn, she subpoenaed Yourhackerz.com, a site that sells passwords to email accounts. *Id* at 167-8; Government Exhibit 14. She subpoenaed the business who owned the site and paypal records – the result being that a paypal account associated with Sharon Thorn. *Id* at 171-177. Someone using the paypal account had purchased passwords for email accounts for Maureen Enger, Ashley Enger, and Patricia Freeman. *Id* at 177-178.[1] Government Exhibit 2-1 summarized the accesses into Maureen Anger's AOL account from IP addresses associated with Mrs. Cioni, based on business records contained in Exhibit 2. *Id* at 182-191. Accesses were also made from Carnival Corporation and other subpoenaed records showed that Elaine Cioni, Sharon Thorn and her daughters Meredith Maginnis and Megan Maginnis were on a Carnival cruise at the time of the accesses. *Id* at 190-193; Government Exhibit 5. JW Marriott records indicated that Sharon Thorn was

[1] The parties stipulated that the computers that store electronic mail messages for AOL, LLC are located in the Eastern District of Virginia. *Id* at 181-182.

registered at the hotel in October 2007. Tran. 12/10/2008 at 8-9; Government Exhibit 6. She forensically examined the hard drives on Mrs. Cioni's work and home computers. *Id* at 11-12. Located on the work hard drive were images of the inbox of Sharon Weiner's email inbox as well as email communications associated with email addresses for Maureen Enger, Ashley Enger, and Bruce Enger ; she also found order confirmations for yourhackers.com website. *Id* at 15-20. She has spoken with Mrs. Cioni ten to twelve times. *Id* at 24. When she first contacted her, in November 2007, she pretended to be an agent from the spoof card company; Mrs. Cioni said she didn't know what the agent was talking about and that she had not authorized her credit card to be used for the account. *Id* at 25-26. She then contacted Mrs. Cioni a few days later saying she was investigating credit card fraud associated with the spoof card account and Mrs. Cioni said she didn't know anything about the calls on the account, that she had never used the spoof card account and that since there were a lot of charges on the account due to building her house, she may not have recognized them on her statement. *Id* at 26-27. SA Born asked her if she knew Mr. Enger and about their relationship; Mrs. Cioni said she worked for him at Long & Foster but she did not want to comment on their relationship. *Id* at 27. Mrs. Cioni also stated something about if something were to go to court and families were in the audience that lives would be ruined. *Id* at 27. She next spoke to Mrs. Cioni in March 2008 when she went to

Chattanooga to interview her; she played two of the calls for her; she did not have a search warrant for the information produced about the spoof call account under May 2008. *Id* at 30, 63. Mrs. Cioni identified her voice and said the call was from her home although the records showed it was from a tracphone. *Id* at 30. The second call was to Mrs. Cioni's work phone and she identified it as being placed by Sha Sha (Sharon Thorn). *Id* at 30-31. She said she was 99% certain of who was behind the calls to Mr. Enger but she would not tell the name of the person. *Id* at 31. She indicated that maybe Sharon Thorn had mailed the envelope to Mr. Enger with the return address from JW Marriott hotel. *Id* at 31. In May or April 2008, Mrs. Cioni told the agent that she have never accessed any accounts associated with Bruce Enger or his family members. *Id* at 32. She identified Mrs. Cioni in the courtroom. *Id* at 33. When she started her investigation, she assumed Craig Scott was the person making the spoof calls. *Id* at 37. Based on the information she provided the government, the first indictment against Mrs. Cioni charged her with two counts of accessing the Long & Foster electronic mail system; there was no evidence she gathered to support those charges and they were dismissed. *Id* at 63-66. Mr. Enger refused to allow Long & Foster to conduct a forensic examination of his work or home computers. *Id* at 68. Mr. Enger was responding to emails sent by Mrs. Cioni up to two days prior to her arrest. *Id* at 73.

Kiersten Camera worked for Long & Foster since January 2006; she previously was Bruce Enger's assistant. *Id* at 120-1. She answered calls on his line where people did not identify themselves; she would repeat her greeting and then hang up if the caller did not identify. *Id* at 122-3. There would be clumps of calls coming in where the caller id showed his old cellphone number. *Id* at 126. She kept track of the date and time of the calls as well as the number on the caller id. *Id.* During the time period of the calls, Mr. Enger was visibly upset about the calls and expressed concern. *Id* at 128.

Catherine Read previously worked at the director of home service connections for Long & Foster. *Id* at 133. She had yahoo personal and business email account with the same password that she had not given to anyone. *Id* at 135-6. She identified Government Exhibit 24-4 and 24-3 as records of her business and personal email accounts. *Id* at 137-140. She had problems in between April and June 2008 accessing her email boxes. *Id* at 141-2.

DEFENSE EVIDENCE

Sharon Thorn lived in Tennessee. Based on her lawyer's advice, she invoked her Fifth Amendment privilege not to answer any further questions. *Id* at 152-3.

Tom Crum was the human resource director at Chattanooga State Technical Community College in Tennessee. *Id* at 154. He supervised Mrs. Cioni for the

past three years when she worked as their benefits coordinator. *Id* at 155. She was an excellent employee. *Id* at 155. In his opinion, she was a truthful and law abiding person; her reputation among the college community was as a truthful and law abiding person. *Id* at 158-160. If the allegations in the case were true, it would not change his opinion. *Id* at 160. He was aware that there were allegations that she used her work computer as part of the charge in the case and that a search warrant had been executed at her office; he was unaware of amy allegations that she had used her work telephone as part of the conduct in the case. *Id* at 161-2. None of the prosecutor's questions caused him to change his opinion. *Id* at 162.

John Crawley was the employment manager at the college and worked with Mrs. Cioni. *Id* at 163. She was a sterling employee. *Id.* He is of the opinion that she is a highly moral individual and very truthful; she has the same reputation in the college community. *Id* at 164-5. He was aware of the substance of the allegations against Ms. Cioni and if true, that would not change his opinion of her. *Id* at 165-6. Even though he worked with her on a daily basis, he was unaware of the allegations that she used her work computer or telephone as part of the charges in this case. *Id* at 166-7. If he learned that she was reading his personal email without his authorization, that would not change his understanding of her reputation for truthfulness.

Rebecca Ahrens worked for Bruce Enger from January 2003 through July 2006. *Id* at 170. He preferred that she not answer his phone or take messages. *Id* at 170, 173. Mr. Enger was pleased with Mrs. Cioni's work and thought she was doing a good job. *Id* at 172. In her opinion, Mrs. Cioni is a truthful and law abiding person. *Id* at 175.

Elaine Cioni currently lives in Tennessee; she previously lived in Northern Virginia from 1989 to 2006; she is married and lives with her husband and her 13 year old son. *Id* at 176-7. Her husband is aware of the charges and they are still together and he was at the courthouse with her. *Id* at 177. She has a bachelor's degree in human services and a master's degree in industrial and organizational psychology; she is one course shy of a certification as an employee benefit specialist. *Id* at 178. She worked in human resources in excess of 25 years; the last 15 years she worked in benefits. *Id* at 178. She worked for Verizon, Rolls Royce, Long & Foster, and Chattanooga State. *Id* at 178-80. She worked at Long & Foster from October 2004 until July 2006. *Id* at 180. She left to work at US Airways. *Id* at 180. She left Long & Foster because she was attracted to her boss, Bruce Enger. *Id* at 180. She insinuated that he was the person she was attracted to and why she was leaving. *Id* at 182. He took her to lunch on her official last day of work and hugged her in the parking lot; when they got back to the office, he gave her the cactus plant. *Id* at 183. She came back and worked Monday and

Tuesday and they agreed to meet Tuesday after work. *Id* at 183. They just talked and he went away to Paris; when he returned, he came for lunch the two year affair started. *Id* at 184. In the beginning, they met almost every other day for a few hours at lunch time. *Id* at 184. After hearing about spoofing on the internet from Lindsay Lohan spoofing Paris Hilton's cell phone and accessing her voicemail, she decided to get an account so she could confirm her suspicions of Mr. Enger's extramarital and extra-mistress activities. *Id* at 185-6. She made the spoof calls because she was hoping to provide an incentive to Mr. Enger to be faithful to his wife. *Id* at 187. She made a lot of calls and it was not the right thing to do but she never threatened to harm Mr. Enger or his wife. *Id* at 187-8. When she heard the fear in Maureen Enger's voice when she called her , spoofing to be calling from her daughter's phone, it was a reality check and she cancelled the account and stopped the activity. *Id* at 188-9. She called him as a male caller because she was hoping to engage him in conversation to reinforce in his mind that he needed to behave when he was traveling. *Id* at 190. Sharon Thorn also made calls and she made some of those calls without her knowledge. *Id* at 193. She accessed Bruce Enger's email account in late 2006 and told him that she had; the relationship continued. *Id* at 193-4. She also tried to access the email of Maureen Enger, Ashley Enger, Catherine Read, Sharon Wiener and Patty Freeman; she was looking for information on other women or men with whom Mr. Enger might be engaged

in extramarital activities. *Id* at 194-5. She had never done anything like this before and it was totally out of character. *Id* at 198. She did not intend to frighten anyone by making the calls. *Id* at 200. She did not open new email messages on Patty Freeman's account. Tran. 12/11/2008 at 27. She bought Patty Freeman's password using her credit card via paypal; she wasn't sure if it was her paypal or Sharon Thorn's paypal account that she used. *Id* at 28-29. She did not tell Sharon upfront what she was doing. *Id* at 29-30. She didn't want a paper trail so her husband would see what she was doing so she asked Sharon if she could use her credit card. *Id* at 31-32. She also never read new mail in Maureen Enger's or Ashley Enger's or Catherine Read's email accounts. *Id* at 33, 35, 36. She sent the letter from Georgetown with the return address for JW Marriott. *Id* at 37; she did not send the letters to Maureen Engler, Sharon sent those. *Id* at 37. She deleted new messages on Bruce Enger and Maureen Enger's voice mail. *Id* at 41. She and Sharon Thorn would use each other's spoof card accounts. *Id* at 42. They made spoof calls on one occasion together – when she heard the fear in her voice. *Id* at 44. Sharon made at least three calls from Mrs. Cioni's 571 cell phone. *Id* at 47. After the call to Maureen, she continued to call Bruce. *Id* at 53. She admitted that she told SA Born that she had never used a spoof card; she did not feel obligated tell the truth to a FBI agent or to disclose that except in a courtroom. *Id* at 57. She realized now that one has to tell the truth to a FBI agent. *Id* at 60. In May, she told

SA Born that she had not accessed Bruce's email and that she was afraid of him and that he may have her put down like all the Congressmen had their girlfriends killed. *Id* at 60-1. She read Catherine Read's email in hopes of finding out the stats of the investigation. *Id* at 64-5. The reason there were so many accesses to the email accounts is because she would keep checking until an email had been read before she would read it; when an email has not been read, it would be in bold type. *Id* at 65. She was absolutely certain that she did not read unopened email because that would clue the person into the fact that someone was reading their email. *Id* at 66.

SUMMARY OF ARGUMENT

The Court erred in denying pretrial motions to suppress evidence where the affidavits in support of search warrants materially excluded information and did not make out the elements of the alleged criminal violations being investigated. The Court also erred in denying multiple motions to dismiss counts of the indictment and the indictment itself when the grand jury process was corrupted, the indictment failed to allege an offense, failed to alleged a federal offense, violated the Commerce Clause, and violated the Double Jeopardy Clause of the Fifth Amendment in that each count charged her twice with a single offense.

At trial, the Court erred in prohibiting cross examination under Rule 412 when the case did not involved sexual misconduct. The Court also erred in denying the motion for a judgment of acquittal when there was no evidence of appellant's intent to harm, reading opened emails, computer services not giving authorization or any agreement to conspire to access electronic storage.

Finally, the Court imposed an unreasonable sentence during a sentencing hearing wrought with the violation of her right to counsel, Rule 32 and no consideration of the factors under 18 U.S.C. § 3553.

ARGUMENT

1. The Court Erroneously Denied Pretrial Motions

A. Motion to Suppress Evidence from Search Warrants

The Court erroneously denied appellant's motion to suppress evidence seized pursuant to search warrants, finding that the affidavit for a search warrant did not have to make out evidence of all elements of an offense. App 71-73.

Pretrial, appellant moved to suppress computer evidence obtained from the searches executed at her home and office in Chattanooga, Tennessee on May 22, 2008, on grounds that (1) the affidavits in support of the search warrants lacked probable cause to believe that Elaine Cioni had accessed stored wire and electronic communications in violation of Title 18 U.S.C. § 2701 et seq. , and (2) the affidavits intentionally misled the authorizing court and/or demonstrated a reckless disregard for the truth in setting forth the factual allegations in support had been committed.[2]

The affidavits withheld from the magistrate the fact that Ms. Cioni closed her Spoofcard accounts in November 2007, and that Bruce Enger had stopped complaining about receiving this type of call. References to statements by Ms. Cioni's friend, Sharon Thorn, that she knew Ms. Cioni was calling Bruce Enger

[2] Ms. Cioni requested an evidentiary hearing under *Franks v. Delaware*, 438 U.S. 154 (1977).

using a spoof card similarly omit any mention of when she believed Ms. Cioni was making the calls. App. 241. Similarly, information provided by Ms. Thorn about Ms. Cioni's accessing email accounts was either not specific as to time, or dated back to December 2006. App. 241. Statements in the affidavit that two emails sent to the Engers came from Bruce Enger's Long & Foster account omit any mention of when the emails were sent and are pure, unsubstantiated supposition. App. 236. In short, there was no allegation in the affidavits of ongoing criminal activity. Accordingly, the search warrants should have been quashed on the grounds of staleness. *Compare United States v. Farmer*, 370 F.3d 435 (4th Cir. 2004) (large-scale counterfeiting operation unlikely to have been suddenly abandoned even though latest information in the affidavit was nine months before the warrant was issued). The question of staleness depends upon the facts and circumstance of the case, including the nature of the unlawful activity alleged, the length of the activity, and the nature of the property to be seized. *Id.* at 439. Here, none of the circumstances set out in the affidavits point toward a finding of probable cause.

The affidavits also withheld from the magistrate facts easily discernible from the Spoofcard records in Agent Born's possession the facts that: (1) of the "spoof" calls at issue, twenty-six were made from telephone numbers associated with Ms. Cioni, to telephone numbers associated with Ms. Cioni, and (2) a significant

number of the calls made to Bruce Enger's voicemail were hang-ups and not harassing calls. As significantly, the affidavits did not disclose the fact that Bruce Enger had previously forgiven Ms. Cioni for accessing his personal email account. Agent Born was told by Mr. Enger during the course of the investigation that in 2006, when Enger tried to end his personal relationship with Ms. Cioni, Ms. Cioni disclosed to him that she had accessed his personal email account. App. 265. Enger continued his personal relationship with Cioni until August 2007. Taken together, the affidavits included materially misleading and stale information necessary to the finding of probable cause thereby entitling Ms. Cioni to an evidentiary hearing. Although there is a "presumption of validity" with respect to affidavits in support of search warrants, a defendant is entitled to a hearing on the validity of the search warrant affidavit "where the defendant makes a substantial preliminary showing that a false statement made with reckless disregard for the truth was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause. *Franks v. Delaware*, 438 U.S. at 155-56.

It is precisely because 18 U.S.C. § 2701, only proscribes unauthorized access to a voicemail or email message that is stored in intermediate storage temporarily, after the message is sent by the sender, but before it is retrieved by the intended recipient that Counts 2 and 3 of the Indictment specifically allege that Ms.

Cioni gained unauthorized access to "unopened" voicemail (Count 2) and email (Count 3) messages. A warrant application must demonstrate probable cause to believe that a crime has been committed and enumerated evidence of the offense will be found a the place to be searched. In the absence of any allegation that the voicemails and emails were "unopened," the affidavits do not allege a violation of 18 U.S.C. § 2701 and, at least with respect to these facts, do not provide probable cause to believe that evidence of the Computer Storage Act will be found at the locations searched. Mrs. Cioni therefore asks that this Court reverse the order of the Court and grant the suppression of the evidence seized pursuant to the search warrants in this case.

B. Motion to Dismiss Indictment based on Grand Jury Improprieties

The Court also erroneously denied the appellant's motion to dismiss the Indictment on grounds that the government engaged in misconduct or deliberately misinformed the grand jury resulting in her indictment based entirely on mistaken evidence. The original motion was denied by the Court on September 9, 2008. App. 70-71. Appellant than renewed this motion after disclosure of the *Jencks* for SA Born showed that the superseding indictment was based in its entirety on SA Born's testimony at the grand jury of a reading of the requested indictment and again denied by the Court. App. 78-81. The Fifth Amendment 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. The right to indictment guards persons from wrongful prosecution where they are falsely accused. *United States v. Calandra*, 414 U.S. 338, 343 (1974) (grand jury historically protects citizens against unfounded criminal prosecutions). The Fifth Amendment grand jury right is intended to serve "a vital function . . . as a check on prosecutorial power." *United States v. Cotton*, 535 U.S. 625, 634 (2002). The grand jury's historic functions include "both the determination whether there is probable cause to believe a crime has been committed and the protection of citizens against unfounded criminal prosecutions." *United States v. Calandra*, 414 U.S. 338, 343 (1974). Accordingly, the grand jury is "meant to be an independent check on the ability of the government to bring criminal charges against individuals." *In re U.S.*, 441 F.3d 44, 57 (1st Cir. 2006); *see also United States v. Suarez*, 263 F.3d 468, 481 (6th Cir. 2001) (grand jury is a "defendant's main protection against the ringing of unfounded criminal charges"). Moreover, the grand jury's "extraordinary powers of investigation" include the powers to "direct[] its own efforts" and to "determine alone the course of its inquiry." *United States v. Sells Eng'g*, 463 U.S. 418, 423 (1983).

Prosecutorial abuse of the grand jury results in relief when the abuse is prejudicial to the defendant. *See Bank of Nova Scotia v. United States*, 487 U.S. 250, 254 (1988); *see also United States v. Derrick*, 163 F.3d 799, 808 (4th Cir.

1998) (holding that an indictment may not be dismissed based on prosecutorial misconduct, absent a showing of prejudice to the defendant). "[D]ismissal of the indictment is appropriate only 'if it is established that the violation substantially influenced the grand jury's decision to indict' or if there is a 'grave doubt' that the decision to indict was free from the substantial influence of such violations." *Bank of Nova Scotia*, 487 U.S. at 256 (*quoting United States v. Mechanik*, 475 U.S. 66, 78 (1986)).

In *Bank of Nova Scotia*, the Court upheld the reinstatement of the indictment, noting the absence of a history of "prosecutorial misconduct spanning several cases that is so systematic and pervasive as to raise a substantial and serious question about the fundamental fairness of the process." *Id.* at 259. The alleged acts of misconduct were: (1) calling witnesses solely to assert their Fifth Amendment privilege; (2) gathering evidence for civil suits; (3) giving unauthorized oaths to IRS agents; (4) producing misleading, inaccurate summaries; (5) granting of pocket immunity; and (6) permitting two agents to read in tandem before the grand jury. *Id.* at 260. These acts were determined to be "isolated episodes" in the course of a 20-month investigation that did not affect the charging decision. *Id.* at 263. Here, where no other actual evidence presented to the grand jury and the proposed superseding indictment was simply read by the Special Agent to the grand jury, this prosecutorial misconduct did rise to the level of

prejudicing Mrs. Cioni's right to be indicted by the Grand Jury. Here, there must be grave doubt that if there is grave doubt that the decision to indict was free from the substantial influence of this violation. *See id* at 256. As such, this court should reverse the decision of the Court below and remand this case with an order to dismiss the indictment obtained in this case.

C. Motions to Dismiss Counts and Indictment

Appellant also moved to dismiss Counts 1-4[3] on grounds that they failed to allege an offense and violated the Double Jeopardy Clause of the Fifth Amendment in that each count charged her twice with a single offense. Docket Entry #51 Appellant also moved to dismiss the superseding indictment on the grounds that it failed to state a federal offense and violated the Commerce Clause. Docket Entry #54. Both of these motions were erroneously denied by the Court. See Order, 11/6/2008 (Docket Entry #64).

These counts fail to allege an offense and are multiplicitous in that each count charged her twice with a single offense. The constitutional guaranty established by the Double Jeopardy Clause protects against multiple punishments for the same offense. *United States v. Halper*, 490 U.S. 435, 440 (1989). In the multiple punishment context, the interest protected by the Double Jeopardy Clause "is limited to ensuring that the total punishment did not exceed that authorized by

[3] Count 3 was dismissed by the government prior to trial.

the legislature." *United States v. Martin*, 523 F.3d 281, 290 (4th Cir. 2008), *quoting Jones v. Thomas*, 491 U.S. 376, 381 (1989). The protection services principally as a restraint on courts and prosecutors. *See Martin*, 523 F.3d at 290 (noting that "the root of the impact of the Double Jeopardy Clause on the legislature is the principle that the power to define criminal offenses and prescribe punishments upon those found guilty of them belongs solely to the legislature").

The longstanding test for multiplicity of charges was set down in *Blockburger v. United States*, 284 U.S. 299 (1932): "the applicable rule is that where the same act or transaction constitutes a violation of two distinct statutory provisions, the test to be applied to determine whether there are two offenses or only one, is that each provision requires proof of an additional fact which the other does not." Id. at 304. However, the Supreme Court made the point that the Blockburger rule is often easier to state than to apply when a splintered majority of the Supreme Court could not agree on how the test should be effectuated. *See United States v. Dixon*, 509 U.S. 688 (1993). While the Blockburger test focuses on the elements required to be proven under the applicable statutes, and not on the actual allegations in the indictment, see *United States v. Terry*, 86 F.3d 353, 356 (4th Cir. 1997), it is primarily a rule of statutory construction, and does not govern if the analysis is overcome by a clear indication of contrary legislative intent. *Abernaz v. United States*, 450 U.S. 333, 340 (1981). In a case interpreting

congressional intent in the context of a *Blockburger* analysis, the Fourth Circuit recently instructed that "Congress ordinarily does not intend to punish the same offense under two different statutes. Accordingly, where two statutory provisions proscribe the 'same offense.' They are construed not to authorize cumulative punishments in the absence of a clear indication of contrary legislative intent." (citation omitted). *United States v. Martin*, 523 F.3d at 290. Only if the statute provides no definitive indication of congressional intent do courts apply the rule of statutory construction prescribed by the Supreme Court in *Blockburger*. *Id*.

Given this framework, examination of the two provisions the accused is alleged to have been violated show that appellant's rights have been violated here. Title 18 U.S.C. § 1030(a)(2)(C) proscribes intentionally accessing (or attempting to access) a protected computer, without authorization, and thereby obtaining information from a protected computer, if the conduct involves an interstate or foreign communication. The term "protected computer" includes a computer which is used in interstate or foreign commerce or communication. 18 U.S.C. §1030(e)(2)(B). The punishment for an offense under subsection (a)(2) is a fine, or imprisonment for not more than one year, or both. §1030 (c)(2)(A). However, the punishment for an offense under subsection (a)(2) is a fine or imprisonment for not more than five years, or both, if the offense was committed in furtherance of any

criminal or tortious act in violation of the Constitution or laws of the United States or of any state. §1030 (c)(2)(B) (ii).[4]

Title 18 U.S.C. §2701(a) proscribes intentionally accessing, without authorization, a facility through which an electronic communication service is provided and thereby obtaining access to electronic communications while it is in electronic storage (unopened). A provider of email accounts over the Internet is a provider of electronic communication service. *See* 18 U.S.C. § 2510(15); *see also FTC v. Netscape Communications Corp.*, 196 F.R.D. 559, 560 (N.D.Cal.2000). If the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortuous act in violation of the Constitution or laws of the United States or any State, the punishment for an offense under subsection (a)(2) is a fine or imprisonment for not more than five years, or both. § 2701(b)(1)(A). In any other case, the punishment for an offense under subsection (a)(2) is a fine or imprisonment for not more than one year, or both. § 2701(b)(2)(A). Thus, in the case of both statutes, felony charges require proof of an additional element: that the accused acted "for commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act." This

[4] §1030 (c)(2)(B) also makes the punishment of an offense under subsection (a)(2) punishable by as a for not more than five years is the offense was committed for the purposes of commercial advantage or private financial gain, see §1030 (c)(2)(B)(I) or, the value of the information obtained exceeds $5000, see §1030 (c)(2)(B)(iii).

element was added to Section 2701 by the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

Clearly, to increase the punishment from one to five years, the prohibited purpose must be the accused's primary motivation or at least a determinative factor in the accused's motivation. *See United States v. Cassiere,* 4 F.3d 1006, 1021 (1st Cir.1993). It should be obvious beyond peradventure that the prohibited purpose harbored by the accused must be a purpose other than the accessing of unlawfully accessing stored electronic communications. The Department of Justice Computer Crime & Intellectual Property Section Manual recognized this precept stating that:

> "Naturally, the 'in furtherance of any criminal or tortious act' language means an act other than the unlawful access to stored communications itself. See *Boddie v. American Broadcasting Co.,*731 F.2d 333, 339 (6th Cir. 1984)." (emphasis added).[5]

That is precisely what the indictment in this case purports to do.

It should be equally clear that *Blockburger* cannot be satisfied simply by the use of different, although technically indistinguishable statutory terms. It is clear that in the circumstances of this case, the parallel elements of § 1030 and § 2701 are indistinguishable for the purposes of *Blockburger*. Consequently, the Court is required to conclude that, as alleged in the Superseding Indictment, § 1030 does not require proof of a fact distinct from § 2701 and cannot serve as the separate

[5] The CCIPS Manual can be accessed at http://www/cybercrim.gov/ccmanual/01ccma.html.

and distinct prohibited purpose and vice versa. Moreover, even if the accused were to concede a hypothetical difference in the elements of the two crimes, "the [*Blockburger*] rule should not be controlling where, for example, there is a clear indication of contrary legislative intent." *Missouri v. Hunter*, 459 U.S. 359, 367 (1983). Requiring proof in both statutes of an additional element in order to elevate a misdemeanor offense to a felony is a clear indication of action by the prosecution in this case absolutely contrary to the legislative intent. As such, these Counts should have been dismissed. Appellant urges the Court to reverse the judgment on counts 1,2 and 4 and dismiss these counts or in the alternative, remand the matter for entry of judgment on the lesser included misdemeanor charges.

The Court below also erred in denying the motion to dismiss the indictment based because it failed to state a federal offense and violated the Commerce Clause. In *United States v. Lopez*, 514 U.S. 549 (1995), the Supreme Court of the United States invalidated the Gun-Free School Zones Act ("GFSZA") because it did not regulate a commercial activity, and therefore exceeded Congress's authority under the Commerce Clause, U.S. Const. Art. I, § 8, cl.3. Five years later, in *United States v. Morrison*, 529 U.S. 598 (2000), the Court struck down the Violence Against Women Act, as another improper attempt to, through the Commerce Clause, federally control criminal activity that did not substantially

involve interstate commerce. The charges against Ms. Cioni pursuant to 18 U.S.C. §1030 (computer intrusion), 18 U.S.C. § 2701 (unlawful access to stored communications), and 47 U.S.C. § 223 (harassing telephone calls) are unconstitutional on the same grounds as those found by the Court in *Lopez* and *Morrison*.

In *Lopez*, the Court held that there are "three broad categories of activity that Congress may regulate under its Commerce Power," including "the use of the channels of interstate commerce . . . the instrumentalities of interstate commerce . . . and those activities bearing a substantial relation to interstate commerce." 514 U.S. at 557. Specifically, the Court held that the GFSZA, which criminalized the possession of guns within a school zone, "has nothing to do with 'commerce' or any sort of economic enterprise, however broadly one might define those terms," and that it was "not an essential part of a larger regulation of economic activity, in which the regulatory scheme could be undercut unless the intrastate activity were regulated." *Id*. at 561. Similarly, the *Morrison* Court, relying heavily on *Lopez*, held that "gender-motivated crimes of violence are not, in any sense of the phrase, economic activity. . . . thus far in our Nation's history our cases have upheld Commerce Clause regulation of intrastate activity only where that activity is economic in nature." 529 U.S. at 611. In illustrating how regulating possession of a gun in a school zone does not affect interstate commerce, the *Lopez* Court

enumerated examples of statutes in which regulating *intrastate* economic activity does, in fact, have a subsequent affect on *interstate* commerce. The Court concluded that the possession of guns within a school zone was a criminal activity of the sort that is usually and properly regulated by the state: "[t]o uphold the Government's contentions here, we would have to pile inference upon inference in a manner *that would bid fair to convert congressional authority under the Commerce Clause to a general police power* of the sort retained by the States." *Id*. at 567. (Emphasis added.) (*See also* Kennedy, J., concurring) ("Were the Federal Government to take over the regulation of entire areas of traditional state concern, areas having nothing to do with the regulation of commercial activities, the boundaries between the spheres of federal and state authority would blur and political responsibility would become illusory.) Similarly, as applied to the facts either alleged in the Superseding Indictment or those established at trial, none of the activities that Congress attempts to regulate in §§ 1030, 2701 or 223 has a substantial nexus to interstate commerce.

On the facts established at trial in this case, the statutes as charged to not reflect a legitimate federal interest, and are not even arguably a "part of a larger regulation of economic activity" see *Lopez*, 514 U.S. at 561, a position that is further supported by the government's decision not to charge Ms. Cioni's unindicted co-conspirator, Sharon Thorn who the discovery establishes engaged in

identical conduct with additional unrelated "victims". Therefore, appellant requests that this Court reverse the decision of the trial court and dismiss the indictment in this case.

2. Exclusion of Evidence under Federal Rule of Evidence 412

At trial, defense counsel attempted to cross examine the chief witness Bruce Enger concerning his misleading of other women with whom he had also had affairs. App 82-84. This was relevant because it went to his veracity. The court excluded this evidence under Federal Rule of Evidence 412, which simply has not applicable here. *See Addendum.* This was not a case where sexual misconduct was charged. As such, this was erroneous and such cross examination should be allowed at a new trial.

3. Motion for a Judgment of Acquittal

The trial court erred in denying the motion for a judgment of acquittal. This motion was preserved at the close of the government's case, Tr. 12/10/08 at 149-50, written memorandum was submitted, Docket Entry #110, argument was made, Tr. 12/11/08 at 1-23 and a post trial motion was also filed, Docket Entry #125, and argued. App. 111-125. This Court reviews de novo a district court's denial of a motion, made pursuant to Rule 29 of the Federal Rules of Criminal Procedure, for judgment of acquittal. *United States v. Alerre*, 430 F.3d 681, 693 (4th Cir. 2005).

Here, this Court should reverse the ruling of the trial court and enter judgment of acquittals on all counts.

A. The government offered no evidence of an agreement between the defendant and any other person to access protected computers owned by AOL or any other internet service provider and obtain emails. Nor did the government offer any evidence of an agreement between the defendant and any other person to do so in furtherance of the offense of accessing AOL or any other internet service provider to obtain unopened emails. As such, the Court should enter a judgment of acquittal on Count 1.

B. The evidence on Counts 1, 2 and 4 was insufficient to establish that Mrs. Cioni violated §1030(A)(2)(C) in furtherance of a violation of § 2701. The government offered no evidence that the defendant acted with the intent or purpose to gain access to "unopened emails" – a necessary element of § 2701. The term "in electronic storage" is narrowly defined in 18 U.S.C. § 2510(17) and refers only to temporary storage, made in the course of transmission, by a provider of electronic communications service. If the communication has been accessed, i.e., opened, by a recipient, it is no longer in "electronic storage." *Fraser v. Nationwide Mutual Insurance Co.*, 135 F. Supp. 2d 623, 634-638 (E.D. Pa. 2001) The government offered no evidence that any of the emails that the defendant

accessed or attempted to access had not be previously read (opened) by their intended recipients. As such, the Court should enter judgment of acquittal on counts 1-2, 4 and 6.

C. The government presented no evidence that Ms. Cioni's access or attempted access was not authorized by the owners of the "protected computers" and "electronic communications services," who are the internet service providers and not the email account holders. As such, the Court should enter judgment of acquittal on counts 1-2, 4 and 6.

D. The government presented no evidence that Mrs. Cioni's access to voice mail was in furtherance of harassing phone calls. There was no evidence of any nexus between the two alleged acts of listening to voice mails and making harassing calls. As such, the Court should enter a judgment of acquittal on count 6.

E. A violation of §1030(a)(2) is generally a misdemeanor. 18 U.S.C. § 1030(c)(2)(A). However, when § 1030(a)(2) is violated "in furtherance of" another crime, it becomes a felony punishable by up to five years imprisonment. 18 U.S.C. § 1030(c)(2)(B)(ii).[6] The Counts 1, 2 and 4 of the Indictment charges violations of

[6] *See United States v. Czubinski*, 106 F.3d 1069, 1079 ((1997)(stating that "[t]he broad language of the mail and wire fraud statutes are both their blessing and their curse. They can address new forms of serious crime that fail to fall within more specific legislation. *United States v. Maze*, 414 U.S. 395, 405-06, 38 L. Ed. 2d 603, 94 S. Ct. 645 (1974) (observing that the mail fraud statute serves "as a first line of defense" or "stopgap device" to tackle new types of frauds before

§ 1030(a)(2), (or a conspiracy to violate § 1030(a)(2), and then seeks a felony enhancement by a violation of § 2701, a statute which prohibits the same conduct as section 1030(a)(2). When Congress enacted the 1996 amendments to18 U.S.C. § 1030(a) of the Computer Fraud and Abuse Act, P.L.104-292, 110 Stat. 3488, it provided a clear indication of its intention to limit the meaning of the term "for the purpose of committing any criminal or tortious act." That legislative intent is contained in Senate Report (Judiciary Committee) No. 104-357, August 22, 1996, accompanying S. 982.

Senate Report No. 104-357 described the proposed amendments to subsection 1030(a)(2)(C) as "intended to protect against the interstate or foreign theft of information by computer" extending the coverage of § 1030(a)(2) to information held on federal government computers and to computers used in interstate or foreign commerce or communications, if the conduct involved and interstate or foreign communication. The Senate Report also clarifies the drafters' intention with respect to how the offense is punished. Specifically, the Senate Report states:

> The seriousness of a breach in confidentiality depends, in considerable part, on the value of the information taken, or what is planned for the information after it is obtained. Thus the statutory penalties are

---

particularized legislation is developed) (Burger, C.J., dissenting). On the other hand, they might be used to prosecute kinds of behavior that, albeit offensive to the morals or aesthetics of federal prosecutors, cannot reasonably be expected by the instigators to form the basis of a federal felony.")

> structured to provide that obtaining information of minimal value is only a misdemeanor, but obtaining valuable information, or misusing information in other more serious ways is a felony.
>
> The sentencing scheme for section 1030(a)(2) is part of a broader effort to ensure that sentences for section 1030 violations adequately reflect the nature of the offense. Thus, under the bill, the harshest penalties are reserved for those who obtain classified that could be used to injure the United States or assist a foreign state. Those who improperly use computers to obtain other types of information – such as financial records, nonclassified Government information, and information of nominal value from private individuals or companies – face only misdemeanor penalties, unless the information is used for commercial advantage, private financial gain or to commit any criminal or tortious act. For example, individuals who intentionally break into, or abuse their authority to use, a computer and thereby obtain information of minimal value of $5,000 or less, would be subject to a misdemeanor penalty. The crime becomes a felony if the offense was committed for purposes of commercial advantage or private financial gain, for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State, or if the value of the information exceeds $5,000.
>
> The terms 'for purposes of commercial advantage or private financial gain' and 'for the purpose of committing any criminal or tortious act' are taken from the copyright statute (17 U.S.C. 506(a)) and the wiretap statute (18 U.S.C. 2511(1)(d)), respectively, and are intended to have the same meaning as in those statutes."

S.R. 104-357.

Congress has made clear its intention that the violations of §1030 not be punished as a felony where the crime charged is accessing (or attempting to access) personal email accounts and obtaining (or attempting to obtain) personal email in furtherance of the interception itself, i.e., accessing (or attempting to access)

personal email accounts and obtaining (or attempting to obtain) opened or unopened personal email.[7]

In addition to protecting against subsequent prosecutions for the same offense, the Double Jeopardy Clause protects against multiple punishments for the same offense. *North Carolina v. Pearce*, 395 U.S. 711, 717 (1969); U.S. Const. amend. V. By extension, the Double Jeopardy Clause protects against duplicitous and enhanced punishments for the same offense. The mere fact that two

[7] The Department of Justice's own manual on prosecuting computer crimes confirms that the criminal or tortious act used to enhance a penalty must be a *separate* act: "Naturally, the 'in furtherance of any criminal or tortious act' language means an act *other than* the unlawful access to stored communications itself." Computer Crime & Intellectual Property Section, U.S. Dep't of Justice, *Prosecuting Computer Crimes* 82 (Feb. 2007) (*citing Boddie v. American Broadcasting Co*., 731 F.2d 333, 339 (6th Cir. 1984)). In addition, the Department notes in its manual that "the 'in furtherance of" language is taken from the Wiretap Act, see 18 U.S.C. § 2511(2)(d), and that at least one appellate court has stated that this enhancement is operative only when a prohibited purpose is the subject's *primary* motivation or a determinative factor in the subject's motivation. *Id*. at 82 (citing *United States v. Cassiere*, 4 F.3d 1006, 1021 (1st Cir. 1993)). An offender's motivation is not the end of the inquiry: *when* the offender formed the requisite motivation is central to whether the "in furtherance of" enhancement applies. The motivation must have been formed in anticipation of committing the additional crime, and sustained long enough to have caused harm." For example, the manual states, "in *By-Prod Corp. v. Armen-Berry Co*., 668 F.2d 956 (7th Cir. 1982), the Government alleged that the defendant intercepted a telephone call in order to "commit an act that is criminal or tortious under federal or state law." *Id*. The Seventh Circuit held that even if the Defendant formed the requisite intent to use the intercepted tape recording, his failure to actually use the recording was what mattered, because his wrongful intention was not sustained. We doubt [] that a tape recording which was never used could form the basis for liability . . . . It would be a dryly literal reading of the statute that found a violation because at the moment of pressing the "on" button a party to a conversation conceived an evil purpose though two seconds later he pressed the "off" button and promptly erased the two seconds of tape without even playing it back. **A statute that provides for minimum damages of $1000 per violation must have more substantial objects in view than punishing evil purposes so divorced from any possibility of actual harm**. *Id*. at 959-60 (emphasis added). See also *Stockler v. Garrett*, 893 F.2d 856 (6th Cir. 1990) (holding that 'interception' and not 'use' is all that is required to violate Wiretap Act, but failing to abrogate Boddie's holding that the criminal or tortious purpose must be 'other than" the interception and/or use).'"

convictions are authorized by different statutory provisions does not establish clear legislative intent that Congress specifically authorized cumulative punishment for the same conduct. See *Rutledge v. United States*, 517 U.S. 292 (1996); *Williams v. Singletary*, 78 F.3d 1510 (11th Cir. 1996) (no clear indication of legislative intent to authorize cumulative conviction and sentences because no clear language in statute and no indication from state courts or legislature as to how to interpret state law). Therefore the felony enhancements in Counts 1, 2, and 4 should be dismissed as a matter of law.

4. Sentencing Issues

A. Denial of right to counsel[8] for sentencing

As stated in *Brewer v. Williams*, 430 U.S. 387 (1977) the rights granted by Sixth Amendment right to effective assistance of counsel "mean at least that a person is entitled to the help of a lawyer at or after the time that judicial proceedings have been initiated against him, whether by formal charge, preliminary hearing, indictment, information, or arraignment." 430 U.S. at 398. "Although a defendant may waive his right to counsel, the courts entertain every reasonable presumption against the waiver of this fundamental constitutional right." *United States v. Johnson*, 659 F.2d 415, 416 (4th Cir. 1981). "In order for a

[8] Determination of a waiver of the right to counsel is a question of law, and thus we review it de novo." *United States v. Singleton*, 107 F.3d 1091, 1097 n.3 (4th Cir. 1997) (citation omitted).

waiver to be valid, it must be shown that the defendant intentionally relinquished a known right." *Id*. Thus, "[w]aiver of the right to counsel, as of constitutional rights in the criminal process generally, must be a 'knowing, intelligent ac[t] done with sufficient awareness of the relevant circumstances.'" *Iowa v. Tovar*, 541 U.S. 77, 81, 124 S. Ct. 1379, 158 L. Ed. 2d 209 (2004) (*quoting Brady v. United States*, 397 U.S. 742, 748, 90 S. Ct. 1463, 25 L. Ed. 2d 747 (1970)). And it is the government's burden to prove that Venable waived his right to counsel. *See Brewer v. Williams*, 430 U.S. 387, 404, 97 S. Ct. 1232, 51 L. Ed. 2d 424 (1977).

Here, after trial, counsel for Mrs. Cioni withdrew citing "irreconcilable differences which have now and will in the future prevent the undersigned from providing Ms. Cioni with constitutionally guaranteed effective assistance of counsel." Docket Entry #148, *Motion to Withdraw as Attorney* at 2. Mrs. Cioni also requested to proceed *pro se*. Docket Entry #147, *LETTER MOTION to proceed pro se*. At a hearing on this motion, the trial court inquired of Mrs. Cioni's understanding of the sentencing guidelines, to which Mrs. Cioni indicated that the real reason she wanted to go forward without an attorney was because she could not afford to retain one, that her family was practically broke and she could not work any longer with trial counsel. App 129. The trial court found that since she had money in her 401(k), she would not be declared indigent. App. 130. Previously though, the same trial court had appointed counsel to Mrs. Cioni. App

49-52. That counsel had withdrawn when Mrs. Cioni retained trial counsel. App 52. The court refused to appoint counsel for sentencing and forced Mrs. Cioni to go forward without counsel.[9] App. This was not a valid waiver of Mrs. Cioni's right to counsel for sentencing and the sentence in this matter should be vacated and the matter remanded for a sentencing hearing with counsel for Mrs. Cioni. Here, there was no knowing and intelligent waiver of that right and therefore the sentence in this matter should be vacated and the matter remanded for a full resentencing with counsel to assist Mrs. Cioni.

B. No Resolution of Objections to Presentence Investigation Report

After the first draft of the Presentence Investigation Report was prepared, the United States filed its sentencing memorandum, Mrs. Cioni filed an objection to the findings of the report and filed a request for a hearing, Docket Entry #167 and asked for leave to subpoena witnesses to sentencing, Docket Entry #170. She also requested to be able to present evidence at the sentencing hearing itself. App. 152. The court erred by not allowing Mrs. Cioni to present this evidence. Furthermore, the trial court erred by not following Federal Rule of Criminal

[9] It is bizarre to think that the Court would find that Mrs. Cioni could conduct herself appropriately and represent herself adequately given her previous decision not to represent herself because she was "emotionally unable to represent herself", App 78-81 and her trial testimony over two days which was emotional, non responsive and according to the trial court, apparently bordered on contemptuous of the rules of court. Tr. 12/10/2008 at 197-8 ("If you do not confine yourself to the rules of this court in the presence of this jury, then I am going to have to say something that I don't want to have to say. Now you want the jury to hear your case. You are going to have to follow the rules like everyone else. Do you understand?").

Procedure 32 which provides that a sentencing court must, for any disputed portion of the presentence report or issue in controversy, rule on the dispute or determine that a ruling is unnecessary either because the matter will not affect sentencing, or because the court will not consider the matter in sentencing. The Rule further states that the prescribed determinations must be appended to any copy of the presentence report made available to the Bureau of Prisons. FED. R. CRIM. P. 32(i)(3)(C). This failure of the Court to adhere to the commands of Rule 32 requires a remand of this case. *See United States v. McCants*, 434 F.3d 557 (2006). This was especially aggregious here where Mrs. Cioni was forced to go forward without counsel to assist.

C. The Sentence was Unreasonable Given that the Court Failed to Consider the Sentencing Factors of 18 § 3553(a), of which the Guideline Range is Just One Factor.

Under *United States v. Booker*, 543 U.S. 220 (2005), this court must review the sentence itself for reasonableness, 543 U.S. at 260-61, "in light of the sentencing factors that Congress specified in 18 U.S.C. § 3553(a)." *See Watson v. United States*, 476 F.3d 1020, 1023 (2005); *United States v. Price*, 409 F.3d 436, 442 (D.C. Cir. 2005). In its most recent sentencing pronouncement the Supreme Court forcefully reiterated its holding in *United States v. Booker*, 543 U.S. 220 (2005). The Guidelines range is a “starting point,” not “the only consideration.”

Gall v. United States, 128 S.Ct. 586, 596 (2007)*; see also Rita v. United States*, 127 S. Ct. 2456, 2474 (2007)(Stevens, J., concurring) ("Given the clarity of our holding, I trust that those judges who had treated the Guidelines as virtually mandatory during the post-*Booker* interregnum will now recognize that the Guidelines are truly advisory.")

First, in the district court, the guideline range is not presumptively reliable – in error, the trial court here did not consider the propriety of any sentencing outside of the guidelines range. *See Rita v. United States*, 127 S.Ct. 2456 (2007).

Second, the district court still failed to properly review each of the § 3553(a) factors. 18 U.S.C. § 3553(a). That provision tells the sentencing judge to consider (1) offense and offender characteristics; (2) the need for a sentence to reflect the basic aims of sentencing, namely (a) "just punishment" (retribution), (b) deterrence, (c) incapacitation, (d) rehabilitation; (3) the sentences legally available; (4) the Sentencing Guidelines; (5) Sentencing Commission policy statements; (6) the need to avoid unwarranted disparities; and (7) the need for restitution. The provision tells the sentencing judge to "impose a sentence sufficient, but not greater than necessary, to comply with" the basic aims of sentencing as set out above, not whether the guideline range is sufficient. *Id.* The Court's determination was run by the Guidelines, which under § 3553(a), this is just one of the seven things for the Court to consider. This is an inappropriate analytical framework

since the guidelines are merely one of seven things to consider. Following excision of the Sentencing Guidelines' mandatory provision, *Booker* now "requires judges to take account of the Guidelines together with other sentencing goals." 543 U.S. at 259-60, (citing 18 U.S.C. § 3553(a)).

Finally, the court did not substantively address most of the statutory factors in giving its reason for decision, nor provide analysis of them. The court's mere recitation of the some of factors does not satisfy the requirements § 3553. *See* 18 U.S.C. § 3553(c) ("The court, at the time of sentencing, shall state in open court the *reasons* for its imposition of the particular sentence .... ") (emphasis added); *see also United States v. Simpson,* 430 F.3d 1177, 1186-7 (D.C. Cir 2005). In pronouncing sentence, the district court relied exclusively his guidelines determination. The sentence, lacking consideration of the necessary statutory factors, is insufficient in light of the Supreme Court's decision in *Booker. See United States v. Ayers,* 428 F.3d 312, 314 (D.C. Cir. 2005) (recognizing that *post-Booker,* the sentencing factors acquired renewed significance).

Based on the court's failure to properly consider all of the § 3553(a) factors, Mrs. Cioni’s sentence is unreasonable under *Booker* and her sentence should be vacated and her case remanded to the district court for a full resentencing.

CONCLUSION

For the foregoing reasons, Mrs. Cioni respectfully requests that this Court vacate the pretrial orders and vacate her convictions and remand this matter for a new trial consistent with the issues raised herein. In the alternative, Mrs. Cioni asks that the sentence in this matter be vacated and that the Court remand her case to the district court for resentencing with the appointment of counsel to assist her. Finally, Mrs. Cioni asks in the alternative that the felony counts be vacated and that this matter be remanded for entry of misdemeanor convictions.

Respectfully submitted,

/s/

_____

JENIFER WICKS

The Law Offices of Jenifer Wicks
The Webster Building
503 D Street NW Suite 250A
Washington, D.C. 20001
(202) 393-3004

Appointed by the Court for Appellant

CERTIFICATE OF COMPLIANCE

This brief has been prepared on in 14-point Times New Roman font. This brief contains 13,079 words and complies with the 14,000 word limitation pursuant to Rule 32.

/s/
_____
JENIFER WICKS

CERTIFICATE OF SERVICE

I hereby certify that on July 29, 2010, a copy of the foregoing was served by electronic mail on:

JAY PRABHU
U.S. Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314

/s/
_____
JENIFER WICKS

ADDENDUM

18 U.S.C. § 371. Conspiracy to commit offense or to defraud United States

If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both.

If, however, the offense, the commission of which is the object of the conspiracy, is a misdemeanor only, the punishment for such conspiracy shall not exceed the maximum punishment provided for such misdemeanor.

18 U.S.C. § 1030. Fraud and related activity in connection with computers

(a) Whoever--

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y.[(y)] of section 11 of the Atomic Energy Act of 1954 [42 USCS § 2014(y)], with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $ 5,000 in any 1-year period;

(5) (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.[;]

(6) knowingly and with intent to defraud traffics (as defined in section 1029 [18 USCS § 1029]) in any password or similar information through which a computer may be accessed without authorization, if--

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States; [or]

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any--

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

shall be punished as provided in subsection (c) of this section.

(b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is--

(1)

(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section; or an attempt to commit an offense punishable under this subparagraph;

(2) (A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under

subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if--

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $ 5,000; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)

(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this section;

(4) (A) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of--

(i) an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)--

(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $ 5,000 in value;

(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(III) physical injury to any person;

(IV) a threat to public health or safety;

(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

(VI) damage affecting 10 or more protected computers during any 1-year period; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(B) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 10 years, or both, in the case of--

(i) an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i); or

(ii) an attempt to commit an offense punishable under this subparagraph;

(C) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 20 years, or both, in the case of--

(i) an offense or an attempt to commit an offense under subparagraphs (A) or (B) of subsection (a)(5) that occurs after a conviction for another offense under this section; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(D) a fine under this title, imprisonment for not more than 10 years, or both, in the case of--

(i) an offense or an attempt to commit an offense under subsection (a)(5)(C) that occurs after a conviction for another offense under this section; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(E) if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for not more than 20 years, or both;

(F) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both; or

(G) a fine under this title, imprisonment for not more than 1 year, or both, for--

(i) any other offense under subsection (a)(5); or

(ii) an attempt to commit an offense punishable under this subparagraph.

(5) [Deleted]

(d)

(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title [18 USCS § 3056(a)].

(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section--

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer--

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means--

(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934 [15 USCS § 78o];

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978 [12 USCS § 3101(1) and (3)]); and

(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act;

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means 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;

(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive department enumerated in section 101 of title 5;

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;

(10) the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(11) the term "loss" means any 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; and

(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection [enacted Sept. 13, 1994], concerning investigations and prosecutions under subsection (a)(5).

(i) (1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States--

(A) such person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and

(B) any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

(2) The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any judicial proceeding in relation thereto, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

(j) For purposes of subsection (i), the following shall be subject to forfeiture to the United States and no property right shall exist in them:

(1) Any personal property used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section.

(2) Any property, real or personal, which constitutes or is derived from proceeds traceable to any violation of this section, or a conspiracy to violate this section.

18 U.S.C. § 2701. Unlawful access to stored communications

(a) Offense. Except as provided in subsection (c) of this section whoever--
(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
(2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) Punishment. The punishment for an offense under subsection (a) of this section is--
(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State--
(A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and
(B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and
(2) in any other case--
(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and
(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

(c) Exceptions. Subsection (a) of this section does not apply with respect to conduct authorized--
(1) by the person or entity providing a wire or electronic communications service;
(2) by a user of that service with respect to a communication of or intended for that user; or
(3) in section 2703, 2704 or 2518 of this title [18 USCS § 2703, 2704, or 2518].

18 U.S.C. § 3553 Imposition of Sentence
(a) Factors to be considered in imposing a sentence. The court shall impose a sentence sufficient,
but not greater than necessary, to comply with the purposes set forth in paragraph (2) of this
subsection. The court, in determining the particular sentence to be imposed, shall consider--
(1) the nature and circumstances of the offense and the history and characteristics of the
defendant;
(2) the need for the sentence imposed--
(A) to reflect the seriousness of the offense, to promote respect for the law, and to provide
just punishment for the offense;
(B) to afford adequate deterrence to criminal conduct;
(C) to protect the public from further crimes of the defendant; and
(D) to provide the defendant with needed educational or vocational training, medical care, or
other correctional treatment in the most effective manner;
(3) the kinds of sentences available;
(4) the kinds of sentence and the sentencing range established for--
(A) the applicable category of offense committed by the applicable category of defendant as
set forth in the guidelines--
(i) issued by the Sentencing Commission pursuant to section 994(a)(1) of title 28, United
States Code, subject to any amendments made to such guidelines by act of Congress (regardless
of whether such amendments have yet to be incorporated by the Sentencing Commission into
amendments issued under section 994(p) of title 28); and
(ii) that, except as provided in section 3742(g) [18 USCS § 3742(g)], are in effect on the
date the defendant is sentenced; or
(B) in the case of a violation of probation or supervised release, the applicable guidelines or
policy statements issued by the Sentencing Commission pursuant to section 994(a)(3) of title 28,

United States Code, taking into account any amendments made to such guidelines or policy statements by act of Congress (regardless of whether such amendments have yet to be incorporated by the Sentencing Commission into amendments issued under section 994(p) of title 28);

(5) any pertinent policy statement--

(A) issued by the Sentencing Commission pursuant to section 994(a)(2) of title 28, United States Code, subject to any amendments made to such policy statement by act of Congress (regardless of whether such amendments have yet to be incorporated by the Sentencing Commission into amendments issued under section 994(p) of title 28); and

(B) that, except as provided in section 3742(g) [18 USCS § 3742(g)], is in effect on the date the defendant is sentenced.[;]

(6) the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and

(7) the need to provide restitution to any victims of the offense.

§ 223. Obscene or harassing telephone calls in the District of Columbia or in interstate or foreign communications

(a) Prohibited acts generally. Whoever--
(1) in interstate or foreign communications--
(A) by means of a telecommunications device knowingly--
(i) makes, creates, or solicits, and
(ii) initiates the transmission of,
any comment, request, suggestion, proposal, image, or other communication which is obscene or child pornography, with intent to annoy, abuse, threaten, or harass another person;
(B) by means of a telecommunications device knowingly--
(i) makes, creates, or solicits, and
(ii) initiates the transmission of,
any comment, request, suggestion, proposal, image, or other communication which is obscene or child pornography, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication;
(C) makes a telephone call or utilizes a telecommunications device, whether or not conversation or communication ensues, without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person at the called number or who receives the communications;
(D) makes or causes the telephone of another repeatedly or continuously to ring, with intent to harass any person at the called number; or
(E) makes repeated telephone calls or repeatedly initiates communication with a telecommunications device, during which conversation or communication ensues, solely to harass any person at the called number or who receives the communication; or
(2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity,

shall be fined under title 18, United States Code, or imprisoned not more than two years, or both.

(b) Prohibited acts for commercial purposes; defense to prosecution.
(1) Whoever knowingly--
(A) within the United States, by means of telephone, makes (directly or by recording device) any obscene communication for commercial purposes to any

person, regardless of whether the maker of such communication placed the call; or

(B) permits any telephone facility under such person's control to be used for an activity prohibited by subparagraph (A), shall be fined in accordance with title 18, United States Code, or imprisoned not more than two years, or both.

(2) Whoever knowingly--

(A) within the United States, by means of telephone, makes (directly or by recording device) any indecent communication for commercial purposes which is available to any person under 18 years of age or to any other person without that person's consent, regardless of whether the maker of such communication placed the call; or

(B) permits any telephone facility under such person's control to be used for an activity prohibited by subparagraph (A), shall be fined not more than $ 50,000 or imprisoned not more than six months, or both.

(3) It is a defense to prosecution under paragraph (2) of this subsection that the defendant restricted access to the prohibited communication to persons 18 years of age or older in accordance with subsection (c) of this section and with such procedures as the Commission may prescribe by regulation.

(4) In addition to the penalties under paragraph (1), whoever, within the United States, intentionally violates paragraph (1) or (2) shall be subject to a fine of not more than $ 50,000 for each violation. For purposes of this paragraph, each day of violation shall constitute a separate violation.

(5) (A) In addition to the penalties under paragraphs (1), (2), and (5), whoever, within the United States, violates paragraph (1) or (2) shall be subject to a civil fine of not more than $ 50,000 for each violation. For purposes of this paragraph, each day of violation shall constitute a separate violation.

(B) A fine under this paragraph may be assessed either--

(i) by a court, pursuant to civil action by the Commission or any attorney employed by the Commission who is designated by the Commission for such purposes, or

(ii) by the Commission after appropriate administrative proceedings.

(6) The Attorney General may bring a suit in the appropriate district court of the United States to enjoin any act or practice which violates paragraph (1) or (2). An injunction may be granted in accordance with the Federal Rules of Civil Procedure.

(c) Restriction on access to subscribers by common carriers; judicial remedies respecting restrictions.

(1) A common carrier within the District of Columbia or within any State, or in interstate or foreign commerce, shall not, to the extent technically feasible, provide access to a communication specified in subsection (b) from the telephone of any subscriber who has not previously requested in writing the carrier to provide access to such communication if the carrier collects from subscribers an identifiable charge for such communication that the carrier remits, in whole or in part, to the provider of such communication.

(2) Except as provided in paragraph (3), no cause of action may be brought in any court or administrative agency against any common carrier, or any of its affiliates, including their officers, directors, employees, agents, or authorized representatives on account of--

(A) any action which the carrier demonstrates was taken in good faith to restrict access pursuant to paragraph (1) of this subsection; or

(B) any access permitted--

(i) in good faith reliance upon the lack of any representation by a provider of communications that communications provided by that provider are communications specified in subsection (b), or

(ii) because a specific representation by the provider did not allow the carrier, acting in good faith, a sufficient period to restrict access to communications described in subsection (b).

(3) Notwithstanding paragraph (2) of this subsection, a provider of communications services to which subscribers are denied access pursuant to paragraph (1) of this subsection may bring an action for a declaratory judgment or similar action in a court. Any such action shall be limited to the question of whether the communications which the provider seeks to provide fall within the category of communications to which the carrier will provide access only to subscribers who have previously requested such access.

(d) Sending or displaying offensive material to persons under 18. Whoever--

(1) in interstate or foreign communications knowingly--

(A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or

(B) uses any interactive computer service to display in a manner available to a person under 18 years of age,

any comment, request, suggestion, proposal, image, or other communication that is obscene or child pornography, regardless of whether the user of such service placed the call or initiated the communication; or

(2) knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity,

shall be fined under title 18, United States Code, or imprisoned not more than two years, or both.

(e) Defenses. In addition to any other defenses available by law:

(1) No person shall be held to have violated subsection (a) or (d) solely for providing access or connection to or from a facility, system, or network not under that person's control, including transmission, downloading, intermediate storage, access software, or other related capabilities that are incidental to providing such access or connection that does not include the creation of the content of the communication.

(2) The defenses provided by paragraph (1) of this subsection shall not be applicable to a person who is a conspirator with an entity actively involved in the creation or knowing distribution of communications that violate this section, or who knowingly advertises the availability of such communications.

(3) The defenses provided in paragraph (1) of this subsection shall not be applicable to a person who provides access or connection to a facility, system, or network engaged in the violation of this section that is owned or controlled by such person.

(4) No employer shall be held liable under this section for the actions of an employee or agent unless the employee's or agent's conduct is within the scope of his or her employment or agency and the employer (A) having knowledge of such conduct, authorizes or ratifies such conduct, or (B) recklessly disregards such conduct.

(5) It is a defense to a prosecution under subsection (a)(1)(B) or (d), or under subsection (a)(2) with respect to the use of a facility for an activity under subsection (a)(1)(B) that a person--

(A) has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology; or

(B) has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number.

(6) The Commission may describe measures which are reasonable, effective, and appropriate to restrict access to prohibited communications under subsection (d). Nothing in this section authorizes the Commission to enforce, or is intended to provide the Commission with the authority to approve, sanction, or permit, the use of such measures. The Commission shall have no enforcement authority over the failure to utilize such measures. The Commission shall not endorse specific products relating to such measures. The use of such measures shall be admitted as evidence of good faith efforts for purposes of paragraph (5) in any action arising under subsection (d). Nothing in this section shall be construed to treat interactive computer services as common carriers or telecommunications carriers.

(f) Violations of law required; commercial entities, nonprofit libraries, or institutions of higher education.

(1) No cause of action may be brought in any court or administrative agency against any person on account of any activity that is not in violation of any law punishable by criminal or civil penalty, and that the person has taken in good faith to implement a defense authorized under this section or otherwise to restrict or prevent the transmission of, or access to, a communication specified in this section.

(2) No State or local government may impose any liability for commercial activities or actions by commercial entities, nonprofit libraries, or institutions of higher education in connection with an activity or action described in subsection (a)(2) or (d) that is inconsistent with the treatment of those activities or actions under this section: Provided, however, That nothing herein shall preclude any State or local government from enacting and enforcing complementary oversight, liability, and regulatory systems, procedures, and requirements, so long as such systems, procedures, and requirements govern only intrastate services and do not result in the imposition of inconsistent rights, duties or obligations on the provision of interstate services. Nothing in this subsection shall preclude any State or local government from governing conduct not covered by this section.

(g) Application and enforcement of other Federal law. Nothing in subsection (a), (d), (e), or (f) or in the defenses to prosecution under subsection (a) or (d) shall be construed to affect or limit the application or enforcement of any other Federal law.

(h) Definitions. For purposes of this section--

(1) The use of the term "telecommunications device" in this section--

(A) shall not impose new obligations on broadcasting station licensees and cable operators covered by obscenity and indecency provisions elsewhere in this Act [47 USCS §§ 151 et seq.];

(B) does not include an interactive computer service; and

(C) in the case of subparagraph (C) of subsection (a)(1), includes any device or software that can be used to originate telecommunications or other types of communications that are transmitted, in whole or in part, by the Internet (as such term is defined in section 1104 of the Internet Tax Freedom Act (47 U.S.C. 151 note)).

(2) The term "interactive computer service" has the meaning provided in section 230(f)(2) [47 USCS § 230(f)(2)].

(3) The term "access software" means software (including client or server software) or enabling tools that do not create or provide the content of the communication but that allow a user to do any one or more of the following:

(A) filter, screen, allow, or disallow content;

(B) pick, choose, analyze, or digest content; or

(C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.

(4) The term "institution of higher education" has the meaning provided in section 101 of the Higher Education Act of 1965 [20 USCS § 1001].

(5) The term "library" means a library eligible for participation in State-based plans for funds under title III of the Library Services and Construction Act (20 U.S.C. 355e et seq.).

Federal Rule of Evidence 412. Sex Offense Cases; Relevance of Alleged Victim's Past Sexual Behavior or Alleged Sexual Predisposition

(a) Evidence generally inadmissible.

The following evidence is not admissible in any civil or criminal proceeding involving alleged sexual misconduct except as provided in subdivisions (b) and (c):

(1) Evidence offered to prove that any alleged victim engaged in other sexual behavior.

(2) Evidence offered to prove any alleged victim's sexual predisposition.

(b) Exceptions.

(1) In a criminal case, the following evidence is admissible, if otherwise admissible under these rules:

(A) evidence of specific instances of sexual behavior by the alleged victim offered to prove that a person other than the accused was the source of semen, injury, or other physical evidence;

(B) evidence of specific instances of sexual behavior by the alleged victim with respect to the person accused of the sexual misconduct offered by the accused to prove consent or by the prosecution; and

(C) evidence the exclusion of which would violate the constitutional rights of the defendant.

(2) In a civil case, evidence offered to prove the sexual behavior or sexual predisposition of any alleged victim is admissible if it is otherwise admissible under these rules and its probative value substantially outweighs the danger of harm to any victim and of unfair prejudice to any party. Evidence of an alleged victim's reputation is admissible only if it has been placed in controversy by the alleged victim.

(c) Procedure to determine admissibility.

(1) A party intending to offer evidence under subdivision (b) must --

(A) file a written motion at least 14 days before trial specifically describing the evidence and stating the purpose for which it is offered unless the court, for good cause requires a different time for filing or permits filing during trial; and

(B) serve the motion on all parties and notify the alleged victim or, when appropriate, the alleged victim's guardian or representative.

(2) Before admitting evidence under this rule the court must conduct a hearing in camera and afford the victim and parties a right to attend and be heard. The motion, related papers, and the record of the hearing must be sealed and remain under seal unless the court orders otherwise.