INFORMATION REQUIREMENTS CLEARINGHOUSE
303-721-7500 -- irch@irch.com

Destruction of Hillary Clinton's Email Records During the U.S. Federal Government Investigation -- The Legal and Records Management Implications

by Donald S. Skupsky, JD, CRM, FAI, MIT

SUMMARY

The news wires have been ablaze with stories about Hillary Clinton's private email server and the destruction of emails and records during government investigation. The story reads like a "who done it" novel. Was there a crime committed or was it just a sequence of unfortunate mistakes? Who is guilty -- Clinton, her staff, her attorneys or her third party service provider? This article reviews the legal issues related to the destruction of Clinton's emails and the legal and records management implications arising from using a "private" email system for government business, and reaches several troubling conclusions with legal and political ramifications.

In 2012, the House of Representatives Select Committee on Benghazi began a government investigation, and requested Clinton to provide information related to the incident. From that point forward Clinton and her team were aware of an on-going government investigation. Many emails related to Benghazi were turned over after review, except for some 30,000 emails the Clinton team considered unrelated to the investigation. Some of these remaining emails were destroyed by late 2014 during government investigation. The remainder were destroyed using secure erasure techniques to prevent recovery on March 31, 2015, a few weeks after Clinton and her third-party service provider received a Preservation Order and a Subpoena from the House Select Committee for any records remaining in the email system.

The destruction of records, including emails, during a government investigation, is a felony under the 2002 U.S. Federal obstruction of justice statute 18 United States Code 1519 (18 USC 1519). Federal courts have determined this statute to be constitutional and rejected claims of vagueness. In essence, any person who deliberately destroys records to prevent them from being used in a government investigation (or other legal matter) is subject to up to 20 years' imprisonment (a felony is a crime with potential punishment of over one year in prison) and a fine (up to $250,000 for a felony). Clearly, the law applies to the destruction of Clinton's records during a government investigation. 18 USC §1361 may also apply to the destruction of federal property. At that time, Clinton held those records as a custodian of federal records and property, and not as the government user or "owner" since she was no longer a federal employee, with no authority to destroy federal property. And, these same records were also subject to Freedom of Information Act (FOIA) requests and subsequent civil law suits to force compliance with these unfulfilled requests.

Under a similar fact situation, we would expect that other people would have already been indicted for obstruction of justice and destruction of federal property. Apparently, federal prosecutors and the FBI apply a different standard during a presidential election.

Destruction of Hillary Clinton's Email Records
During the U.S. Federal Government Investigation --
The Legal and Records Management Implications

by Donald S. Skupsky, JD, CRM, FAI, MIT
President, Information Requirements Clearinghouse

The news wires have been ablaze with stories about Hillary Clinton's private email server -- production of some emails during a protracted government investigation and the destruction of other emails which Clinton deemed unrelated to the investigation. While pundits and supporters construe conclusions based on their political affiliation and beliefs, most do not have the knowledge and experience related to destruction of records and recordkeeping systems to clearly identify the legal and recordkeeping issues related to this matter.

This article is not meant as a political tirade, but rather an objective analysis of the laws related to the known facts and recordkeeping issues affecting the outcome. And, the article intends to clear the air regarding the behavior expected by the law during a government investigation (or litigation or audit) related to the destruction of email and other records.

Background

For the last 30 years, I have preached in my writings, seminars and consulting projects that relevant records may not be destroyed during litigation, government investigation or audit. The records management profession and corporate legal departments advocate procedures, generally referred to as "legal holds" that prevent the improper destruction of records during legal actions. During an expert witness engagement, I was asked to read the twenty passages from my 1988 book "Recordkeeping Requirements" that implored readers to not destroy relevant records when litigation, government investigation or audit is in progress, imminent, or even in some cases even foreseeable.

Why is refraining from records destruction at these times so important? Parties destroying records during a legal proceeding may be attempting to influence the outcome. It is now commonly accepted in both the legal community and the general public that destruction of records at these times implies guilt and an attempt to cover it up, and in criminal matters, obstruction of justice. The courts, both state and federal, unanimously require that parties refrain from destroying records and impose fines, penalties and adverse court rulings to ensure that such behavior will not be tolerated. How can justice be done when potential evidence is systematically and deliberately destroyed to prevent its consideration? And, even if those destroyed records and the evidence contained nothing of value, how will the courts and public know that was true without evaluating the material . . . which becomes impossible when it no longer exists. Today, the courts, litigation attorneys, corporate attorneys, information management specialists, officers of organizations, and most others affected by these issues know and accept these principals.

The courts embodied these principles in rules such as the Federal Rules of Civil Procedure, Rule 27(e):

> e) Failure to Preserve Electronically Stored Information. If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

(1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or

(2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:

(A) presume that the lost information was unfavorable to the party;

(B) instruct the jury that it may or must presume the information was unfavorable to the party; or

(C) dismiss the action or enter a default judgment.

Numerous other jurisdictions through rules and court cases have confirmed the same principal. "Spoliation of evidence" is the intentional, reckless, or negligent withholding, hiding, altering, fabricating, or destroying of evidence relevant to a legal proceeding.[1] Such conduct will result in adverse inferences in litigation[2], fines, penalties, dismissal of claim or default judgment.

Sarbanes-Oxley and Obstruction of Justice

During the Enron government investigation in 2001, the investigators subpoenaed records of Arthur Andersen, Enron's auditor and public accountant. When the records were not turned over, a court in 2002 found that Andersen obstructed justice by deliberately deleting those records. The federal statute at that time provided for only a $500,000 fine against Andersen for obstruction of justice. Unfortunately for Andersen, public sentiment also turned against Andersen leading to its dismantlement and bankruptcy, even though the obstruction judgement was later overturned by the U.S. Supreme Court. Further investigation revealed that Andersen destroyed the relevant Enron records as part of its standard records retention program, which should have been halted once litigation started and a subpoena received.

Due to abuses and fraud in financial reporting by Enron and a large number of other publicly held companies, Congress enacted the Sarbanes-Oxley Act in 2002, with the law fully implemented by 2004. In response to Andersen's light penalty for destruction of records during a criminal investigation, Congress also enacted 18 United States Code 1519 (18 USC 1519) as part of Sarbanes-Oxley -- a much tougher obstruction of justice statute with a clear statement of illegal actions and significant penalties:

18 U.S. Code § 1519 - Destruction, alteration, or falsification of records in Federal investigations and bankruptcy

Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.

[1] Black's Law Dictionary. West Publishing Company, 9th Edition. 2009.
2 Adverse inference – if the evidence did exist, it would be unfavorable to the party destroying evidence.

Corporate executives and board members immediately paid attention to this law due to the potential imprisonment for individuals, as opposed to only a corporate fine. Many companies began scrutinizing their policies and procedures related to records retention and destruction of records, and established safeguards to prevent destruction of records during litigation, government investigation and audit.

The Meaning of 18 USC §1519

The new obstruction of justice statute is very clear and concise. Courts subsequently reviewing its provisions have uniformly upheld its constitutionality[3] and rejected claims of vagueness.[4] It clearly addresses the type of records, evidence or objects covered, the conduct that will evoke the penalties of the law, and the penalties that would result from violations:

1. "Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object . . ." The initial phrase of the law addresses both the state of mind for the person who performs those actions and the actions that violates the law.

    a. *State of Mind #1*. The law only covers situations when a person knowingly performs the conduct specified.[5] This does not mean that the person knows the consequences of their actions. Rather, the law uses "knowingly" to identify a person doing a deliberate act versus an act of nature – e.g., flood. The law does care if the person knew the action would obstruct justice or destroy evidence. The first phrase applies every time a person destroys records, conceals information from another, falsifies documents or covers up their actions.

    b. *Actions Covered*. The law specifies a number of actions that could lead to obstruction of justice. In the matter at hand, destruction of email would clearly be covered. However, concealment of the destruction through secure erasure (so the information cannot be retrieved) or cover up of the destruction would also be an offense.

2. ". . . with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case. . ." This second phrase addresses a second state of mind related to the goal of the destruction of records and context in which the destruction could occur:

    a. State of Mind #2. A criminal statute often requires some intent before considering the actions to be criminal. In this case, the "intent" is to destroy the records so that they would not be available for any government investigation and matter.[6] The level of intent could be as deliberate as to "impede" or "obstruct" or just to "influence" an investigation or proper administration of any

---

3 United States v Fumo (2007, ED Pa) 100 AFTR 2d 6902.

4 United States v Yielding (2011, CA8 Ark) 657 F3d 688. United States v McRae (2012, CA5 La) 702 F3d 806. United States v Russell (2007, DC Conn) 639 F Supp 2d 226. United States v Moyer (2010, MD Pa) 726 F Supp 2d 498.

5 United States v Moyer (2010, MD Pa) 726 F Supp 2d 498.

6 Note that the "intent" in 18 USC 1519 is totally different than the "intent" the FBI did not find after investigating Clinton's private email server: " . . . we did not find clear evidence that Secretary Clinton or her colleagues *intended* to violate laws governing the handling of classified information . . ." Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal E-Mail System, July 5, 2016.

matter. There is no need for there to be a current investigation or even a subpoena – ". . . contemplation of any such matter or case". Thus, the intent to not have the emails available for any government purpose is sufficient to evoke the law, regardless of why the emails were destroyed.

b. *Scope.* The statute applies to any matter within the jurisdiction of any United States Federal agency or department, any judicial proceeding for bankruptcy under Title 11 of the United States Codes, or just in contemplation of any such matter or case.[7]

3. *Penalty.* The penalty for violation of this law could be imprisonment for up to 20 years. And, federal guidelines state that a law with a potential penalty of over 1 year in jail is a felony with a potential fine of $250,000 or more.

Thus, under the statute, someone who knowingly destroys emails with the intent to make the emails unavailable for any current or future federal investigation or proceeding is subject to a fine of up to $250,000 and imprisonment for a period not to exceed 20 years.

Was a Government Investigation in Progress?

Clinton had been informed starting in 2012 of the House Select Committee's investigation of Benghazi and received numerous requests for relevant emails, plus she received both a preservation order and subsequently a subpoena. Here is a brief chronology of the email requests as prepared by Representative Jason Chaffetz:[8]

- September 20, 2012: Committee requested from Clinton information (including emails) related to the Benghazi attack.
- December 2, 2014: Committee requested from David Kendall, Clinton's attorney all official records in Clinton's custody.
- March 3, 2015: Committee sent preservations order[9] to Clinton and email service provider use by Clinton.
- March 4, 2015: Committee issued subpoena to Clinton requiring production of four classes of documents related to Benghazi.[10]
- March 9, 2015: Platte River Networks learned of preservation order.
- March 25, 2015: Clinton's team, including attorneys Kendall and Mills, held a conference call with Platte River Networks' engineer responsible for Clinton email server.

---

[7] United States v Yielding (2011, CA8 Ark) 657 F3d 688. United States v Moyer (2012, CA3 Pa) 674 F3d 192. United States v Ionia Mgmt. S.A. (2007, DC Conn) 526 F Supp 2d 319.

[8] Information request dated September 6, 2016 from Jason Chaffetz, Chairman, U.S. House of Representatives, Committee on Oversight and Government Reform to Mr. Treve Suazo, Chief Executive Officer, Platte River Networks, Denver, Colorado regarding the destruction of emails from the Clinton email server they managed for Clinton.

[9] Preservation Order – an order to preserve and protect records, indicating that it is illegal to alter or destroy the records.

[10] https://benghazi.house.gov/sites/republicans.benghazi.house.gov/files/Kendall.Clinton%20Subpoena%20-%202015.03.04.pdf

- March 31, 2015: Platte River Networks created work ticket for deletion of server emails and destroyed all backups and emails using Bleachbit, a secure computer erase software.

Thus, while a government investigation, protective order and subpoena was in effect, Clinton's team selected what they deemed to be relevant documents and destroyed the rest.

The Impact of Using a Private Email System as a Recordkeeping System

The media accounts so far have not addressed the implications of email as unmanaged, co-mingled information. In a normal recordkeeping system, records related to different functions are kept separately, often in separate rooms in a paper-records systems and generally in separate applications in electronic systems. However, both paper and electronic records can be physically together in the same general space, and still be segregated, if they have been indexed or classified into different categories. For example, accounting records can be physically stored in the accounting department or in an accounting software application for accounting records. This accounting software application can be on the same computer servers as other applications for human resources, marketing or manufacturing, when records for those systems are separated from other records by specific software applications. Alternatively, accounting, human resources, marketing and manufacturing records could be store in one electronic document management system by classifying or indexing the records according to the established taxonomy to create a "virtual," but not physical, segregation of records.

In these types of recordkeeping systems, employees make daily decisions as to whether recorded information received or created by the organization are "records" of the organization that must be kept according to the records retention schedule. When something is a record, ideally it would be moved to some type of managed system for the duration of its retention period. It is also through this division of responsibilities that employees working in accounting can continue to determine which documents are records and which are non-records that do not have to be kept. It is also a characteristic of these systems, for example, that enable marketing records to be destroyed according to the organization's records retention program, while tax records (unrelated to marketing) are being audited and human resource records subject to litigation or government investigation.

Clinton provided some emails that her attorneys deemed relevant, after a search of the email servers using keyword searches and some review. On March 27, 2015, David E. Kendall, Williams & Connolly, LLP, attorney for Mrs. Clinton, provided an explanation as to why the review and selection process conformed to requirements under the Federal Records Act[11]:

> . . . the regulations implementing the Federal Records Act provide that "agencies must distinguish between records and nonrecord materials by applying the definition of records . . to agency documentary materials in all formats and media." 36 C.F.R. §1222.12(a) . . . all employees are required to review each message, identify its value, and either delete it or move it to a recordkeeping system." NARA Bulletin 2014-06 . . .

11 Letter from Kendall to Representative Trey Gowdy, U.S. House of Representatives, March 27, 2015. http://democrats-benghazi.house.gov/sites/democrats.benghazi.house.gov/files/documents/2015_03_27_Kendall_to_TG_re_Response_to_March_4_Subpoena.pdf

Under normal conditions, even for private-sector companies, this explanation might be somewhat acceptable – employees must review documents and store records in a recordkeeping system. Then, many of the so-called non-records can be destroyed. But, this explanation fails for several reasons.

1. *Destruction of Non-Records in the Regular Course of Business*. The review of co-mingled records and destruction of non-records should be done in the regular course of business and not during government investigation. Even the NARA bulletin cited by Clinton's attorney anticipates that the employees review records and then identify its value as the emails are received to eliminate non-records and improve efficiency. There was no urgency to destroy even non-records after Clinton had been out of office for over two years.

2. *Email Not a Recordkeeping System*. The NARA bulletin states that records should be transferred to a recordkeeping system. Email is a "tool of communication" and not a recordkeeping system. Apparently, for many years Clinton maintained these records in the email system, precluding access from other government employees with authorization for this information and perhaps reducing the effectiveness of the Department of State after she left.

3. *Custodial Responsibility*. Once Clinton left office in 2013 she had a duty to turn over records to the official Department of State recordkeeping system, even if as she claimed, she had a right to keep them on her private server. From that point on, these were no longer *her* records and she had no right or authority to destroy any government property under 18 USC §1361.

   18 U.S. Code § 1361 - Government property or contracts

   Whoever willfully injures or commits any depredation against any property of the United States, or of any department or agency thereof, or any property which has been or is being manufactured or constructed for the United States, or any department or agency thereof, or attempts to commit any of the foregoing offenses, shall be punished as follows:

   If the damage or attempted damage to such property exceeds the sum of $1,000, by a fine under this title or imprisonment for not more than ten years, or both; if the damage or attempted damage to such property does not exceed the sum of $1,000, by a fine under this title or by imprisonment for not more than one year, or both.

   As such, she had a custodial responsibility to protect and preserve those records, and return them to the custody of government officials, with no right to destroy them herself. Undoubtedly, the value of the emails destroyed would be valued over $1,000 and the destruction of government property treated as a felony because of the huge cost already incurred by the U.S. government to recover these emails and investigation this matter.

4. *Legal Holds*. Once the government investigation began in 2012, Clinton had a legal duty to place a "legal hold" on the entire email server since it contained co-mingled records and on all other records relevant to the Benghazi investigation. The system should have been properly backed up, protected and removed from normal use. The legal hold process is recognized by government and the private sector as the legally-required response to protect record under government investigation or other legal actions.

The failure to instruct the staff and service provider, constitutes a severe breach of legal duty, creating culpability for even "inadvertent" destruction of others with no knowledge of the government investigation, preservation order or subpoena, and certainly for destruction by those with knowledge. Clinton and her team cannot claim ignorance of this standard legal hold procedure and claim they had no technical knowledge and training. She elected to establish a private system, under her control, rather than using the Department of State system which provided the proper controls, procedures and management expected of federal recordkeeping systems. The Federal Records Act and NARA expect federal employees who manage records to know and follow government requirements. Ignorance of this duty and the legal hold procedures is no excuse.

5. *Destruction During Government Investigation*. But, most importantly, because of the government investigation and the co-mingled nature of email, the subsequent destruction of non-record materials could not legally proceed when it did:

    a. Government investigation was in progress.

    b. The emails were co-mingled – relevant and irrelevant emails resided in the same system.

    c. The normal process of segregating records from non-record material or, in this case, separating relevant from non-relevant material could proceed, but non-records or irrelevant material could not be legally destroyed.

If the business and personal emails had been segregated in the normal course of business, prior to government investigation, then the personal emails could or would have been destroyed in the regular course of business under normal organizational policies.

Implications for Destruction of Email During Government Investigation

18 USC §1519 clearly applies to government investigations. In fact, subsequent court decisions indicate that the provision applies even if the matter is likely to be considered in a future government investigation, even if the investigation is not yet started. Thus, the statute would clearly envision an investigation by Congress of the Benghazi attack when Hillary Clinton was Secretary of State, an investigation by the Federal Bureau of Investigation into whether Clinton's private email servers compromised national security and pending Federal Freedom of Information requests for Department of State records in her possession.

A party to an investigation does not get the option to determine according to its own discretion which records are relevant and which are not, and destroy those the party deems not relevant. They may at the request of the other party immediately turn over relevant records, but then must preserve the rest so that the requesting party has the opportunity to determine whether these records are relevant or not. Destruction of these records using secure erase during government investigation clearly violated this statute since the records were knowingly destroyed to prevent their review by another party.

Clinton claimed the right to remove personal emails from the same email system she used for government business. Clearly, if a home computer and private email system is only used for personal

purposes, and not for any government business, the contents of those systems would not be relevant to a government investigation of government business. But, if there was a possibility that any government business was transacted on that private system, then the entire private system would be subject to review as part of the government investigation. In criminal and tax investigations for other people, these "personal computers" have often be seized by the government.

Here the "private system" was actually used for government business and for personal purposes. There is a well-understood and well-accepted legal principal that establishes that an otherwise private system used for business purposes is considered a business system for business-related litigation or government investigation purposes, and records cannot be destroyed from that system unless the matter is concluded or specific permission is granted by the court or investigator. In sum, once litigation, government investigation or audit is in progress or imminent, there is no right to privacy for otherwise private records in a system used for business purposes.

In addition, 18 USC §1519 treats actions to "conceal" and "cover up" as obstruction of justice to the same extent as destruction of records. From 2012 through 2015, the House Select Committee on Benghazi continuously requested emails and records from the Department of State and Clinton. By selecting which records to turn over and failing to turn over some otherwise relevant information, the Clinton team concealed records covered by a government investigation. Even after the destruction of the emails deemed personal, the FBI and others successfully forensically retrieved relevant records that the secure erase failed to obliterate. On December 5, 2014, David E. Kendall, Clinton's Attorney, tried to explain their procedures, claiming they provided all relevant emails and only retained, and later destroyed, non-relevant, personal information.[12] Clinton in numerous public statements insisted that all relevant records were properly turned over.

The ultimate in concealment and cover up occurred on March 31, 2015, when Platte River Networks (PRN), the service provider for the private email server, destroyed the remaining emails on the Clinton email server. In December 2014, Clinton instructed her team to destroy the remaining emails and set a retention of 60 days. Apparently, the PRN engineer "forgot" to follow those instructions until after a March 25, 2015 conference call with Clinton attorneys. The ultimate destruction of that batch of records during government investigation permanently concealed access to most of those emails, followed by repeated cover-ups designed to make access to potentially relevant records impossible.

Summary of the Crime in Simpler Terms

The following questions are designed to summarize the legal and recordkeeping implications of the actions related to destruction of Clinton emails while government investigation was in progress:

1. *Did Clinton conduct government business on a private email server?* Yes. There is no dispute on this issue.

2. *Was it legal for Clinton to conduct government business on a private email server?* No. Maintaining federal government records on a private email service is not permitted by federal recordkeeping requirements nor under the Federal Records Act, although Clinton claimed other

[12] Letter from Kendall to Representative Trey Gowdy, U.S. House of Representatives, March 27, 2015. Ibid.

government officials had used private email systems in the past. All federal government records must be kept according to federal requirements and destroyed only under federal guidelines when permitted by the records retention program. The fact that some previous government officials maintained private recordkeeping systems does not change the conclusion. The federal government has specific requirements for records, including the obligations to respond to FOIA requests, security of confidential documents, etc., which cannot be complied with in a private system.

3. *Was Clinton subject to government investigation?* Yes. A Congressional investigation of Benghazi began in 2012 and there were several private Freedom of Information (FOIA) requests still pending, creating a legal duty to preserve and turn over responsive records.

4. *Did Clinton have a legal duty to protect and preserve the emails?* Yes. Once government investigation began, Clinton had a legal duty to protect and preserve all government records in her possession that related to Benghazi and all co-mingled systems that potentially contained Benghazi records and other non-relevant government and personal records. Under standard recordkeeping procedures, she should have placed a legal hold on all these recordkeeping systems to prevent any destruction or alteration of records. For the co-mingled emails, under a legal hold, no destruction should have occurred even for records her team or attorneys deemed to be not relevant or even non-records.

5. *Once the government investigation started, could Clinton or her team identify and turn over relevant email based on their own criteria and destroy the rest?* No. While selective retention of email that are records and destruction of email determined to be non-records, based on individual discretion, is a normal business function, this activity becomes illegal once litigation, government investigation or audit is in progress or imminent. And, under 18 USC §1519 destruction of emails with the intent to render them unavailable for any matter is a felony. In this case, there were known legal matters in progress.

6. *Once government investigation started, could Clinton legally destroy any information on her email server?* No. Since the server was used for both business and private emails, for legal purposes, the entire server must be treated as a business or government system, and no otherwise private emails in that system could be destroyed until the various matters ended or the opposing party agreed that such emails were not relevant. Neither event took place when the 30,000 emails were destroyed. This is particularly true since the relevant and non-relevant were comingled, as opposed to being kept separately. Any selective destruction would involve judgment and discretion which is suspect and unreliable for a person under investigation. As stated above, a legal hold should have been placed on these records, providing notice to others and preventing destruction during government investigation.

7. *Why could the private emails not be destroyed?* Besides the answers above, the legal system is well aware that a party to a government investigation cannot objectively determine the relevance of the emails even if performing honorably and certainly would destroy unfavorable emails if acting deceitfully. Thus, the emails must be preserved to give the other party the opportunity to determine relevance, and that right is illegally extinguished when the emails are destroyed.

8. *Can a person destroy government records based on their own discretion?* Yes, if you are an authorized federal employee or contractor, provided that litigation, government investigation and audit is not in progress or imminent. During the course of regular business activities, a government employee would normally identify records required to be kept under a records retention program following approved procedures, and then destroy the remaining non-records. In this case, there was a House Select Committee on Benghazi investigation in progress plus other pending Freedom of Information Act request.

9. *Since Clinton was not a federal employee when the records were destroyed, do the same legal and recordkeeping requirements apply?* Yes. Clinton was not a government official at the time these emails were destroyed. Upon leaving office, she became a custodian of federal government records with an affirmative duty to preserve and protect federal property, and a duty to turn over the federal property to designated government representatives. By failing to protect government property in her possession, Clinton may be subject to the fines and penalties under 18 USC §1361.

10. *If records were destroyed by a third party (PRN), would Clinton still be liable?* Yes. Since Clinton remained the custodian of Department of State records, she had an affirmative duty to preserve them on behalf of the Department according to Federal and other legal requirements. The fact that Clinton team members, attorneys and third-party engineers participated in a conference call less than one week before the records destruction, raises the likelihood that they approved the ultimate destruction. Since Clinton engaged these parties to act on her behalf, she cannot claim that they were acting on their own. If the allegations that her team members, attorneys and third-party contractors conspired to obstruct justice by destroying the records prove to be true, they could also be guilty of the actual obstruction of justice or of conspiracy to obstruct justice, and the attorneys could be disbarred for violating the American Bar Association and state Rules of Conduct.[13]

11. *Did Hillary Clinton violate 18 USC §1519 when emails from her private email server were destroyed during government investigation?* Possibly, yes. The statute applies to anyone who deliberately (knowingly) destroyed emails (records) with the intent to destroy them, rendering them unavailable during any investigation or court proceeding. Since legal matters were in progress, there existed a legal duty to keep all potentially relevant emails which extinguished any right to destroy those emails. While she may not have destroyed the records personally, she failed to protect them or place a legal hold on them and someone serving as her agent performed the actual destruction. In December 2014 she did instruct her team to destroy remaining emails after 60 days. And, ultimately, she never halted nor protested again any records destruction. Under 18 USC §1519, Clinton may have concealed and covered up the destruction of records.

12. *Is conviction under 18 USC §1519 a felony?* Yes. A conviction under a federal statute is a felony if the potential penalty is more than one year in prison or a fine over $250,000 or more.

[13] Rule 3.4 of the American Bar Association Rules of Conduct (generally adopted in the states) states: A lawyer shall not . . . (a) unlawfully obstruct another party' s access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value. A lawyer shall not counsel or assist another person to do any such act;

13. *Is it relevant that before March 4, 2015, Clinton had not received a federal subpoena, had not been indicted nor had a court proceeding been initiated for 18 USC §1519 to apply?* No. The statute does not require a subpoena, indictment or court proceeding to pre-date the actions covered by the statute. The statute applies to certain conduct like destruction of records if done to prevent evidence from being available in any government proceeding, in progress or initiated in the future.

14. *So, wouldn't anyone who knowingly destroys records, even under a records retention program, be subject to this statute?* No. When records are destroyed under a records retention program, before litigation, government investigation or audit is initiated or imminent, the destruction is viewed by courts as a legitimate business activity, performed to further business needs (save money, reduce space, improve efficiency, etc.) and not to impede or interfere with any government proceeding. However, even destruction of relevant records under a retention schedule must end when litigation, government investigation and audit begins, is imminent or in a few isolated situations when foreseeable.

15. *Did Hillary Clinton commit a felony?* To be determined. She violated the provisions of at least two felony statutes related to obstruction of justice and destruction of government property, and thus her actions seem to fulfill the requirements for a felony conviction. However, she will only be guilty of a felony if indicted under the statute and a court confirms she violated the law, regardless of penalty.

16. *What would happen to other people who did the same thing as Clinton?* If other people had destroyed emails subject to a government investigation, they would have promptly be charged with obstruction of justice. A presidential candidate, government official or corporate executive should be treated the same and not "let off the hook"

Is Clinton Legally Liable for Destruction of Emails During Government Investigation

Apparently, there are several parties who played a role in the destruction of emails, and the subsequent concealment and cover-up:

- Hillary Clinton
- Clinton Staff Members
- Clinton Attorneys
- Platte River Networks

So far, no definitive information has surfaced incriminating Clinton for the actual destruction. Clearly, she failed in her duty to protect and preserve government records and property once she left office. She directed her staff to create this private email system, operated it as Secretary of State, and failed to return government property when she left office. She also maintained emails and government records on other laptop computers, cell phones, tablets and other electronic devices. Once government investigation began in 2012, and a protective order and subpoena served on her in March 2015, she failed in her affirmative duty to prevent these records from being destroyed. She failed to place a legal hold on the

emails and records, and it appears that she made no statement, took no action or provided no instructions to her staff, attorneys and third party contractor to protect these records and not destroy them.

There is clear evidence indicating she instructed that all remaining emails be destroyed in December 2014. And, there is significant evidence indicating her role in the concealment and cover-up of the destruction. These records were created by Clinton in her role as a high government official, making her responsible for their ultimate preservation and protection.

Clinton Staff and Attorneys appear to have been actively involved in the segregation of the co-mingled emails and misidentifying "private" emails – either deliberately or mistakenly -- that turned out to be "government" emails. As a result, they participated in the destruction process by identifying and designating records that were destroyed during government investigation. They may have also been responsible for the actual destruction of some records that they deemed to be "non-records" prior to December 2014. Quite curious, the March 25, 2015 conference call with the Platte River Networks engineer responsible for the actual destruction on March 31, 2015 may have included instructions to the engineer to destroy records. While the content of that meeting is currently unavailable because the Clinton Attorneys have claimed attorney-client privilege, the timing raises serious concerns that the attorneys instructed the engineer to quickly proceed with destruction. Otherwise, why would they invoke a privilege for someone who has not been their client before, followed by the actual destruction of records six days later?

Clearly, the Platte River Networks engineer destroyed the actual records during a government investigation, while a preservation order and subpoena was in place. During the FBI investigation of the Clinton emails months before, the FBI granted the engineer immunity in order to elicit information for its investigation. Perhaps, during the March 25 conference call, the Clinton attorney confirmed that this immunity extending to future acts, and that he could proceed with the destruction without fear of repercussions. We may never know the truth unless the attorney-client privilege is successfully challenged.

It is unclear whether the investigations in progress will lead to indictments. Based on this review and analysis it appears that Clinton, some of her staff, her attorneys and the PRN engineer could be liable for obstruction of justice and destruction of federal government property – a felony under both laws.

A Word to the Wise

18 USC §1519 is felony statute with a clear set of requirements and harsh penalties. Do not destroy relevant records while litigation, government investigation or audit is in progress. Destruction of records can proceed in clearly unrelated areas under an established, implemented and legally appropriate records retention program. Records covered by litigation, government investigation and audit should be protected under legal holds to prevent their destruction until the matter is resolved.