THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOL. XVIII STLR.ORG FALL 2016

NOTE

OBSTRUCTION OF JUSTICE IN THE DIGITAL AGE: DEFINING THE *ACTUS REUS* OF 18 U.S.C. §§ 1512(C) AND 1519†

Jacob Arber*

* J.D. Candidate 2017, Columbia Law School. I would like to thank Professor Daniel Richman for his guidance in writing this Note and William Palmer for his thorough comments and feedback.

I. INTRODUCTION

Following a series of high profile scandals, Congress enacted the Sarbanes-Oxley Act ("Sarbanes-Oxley" or "the Act") in 2002.[1] The Act sought primarily to "protect investors by improving the accuracy and reliability of corporate disclosures,"[2] but it also contained numerous other provisions, including the creation of "new anti-shredding crimes."[3] These provisions criminalized "alter[ing], destroy[ing], mutilat[ing], or conceal[ing] a record, document, or other object" with the intent to obstruct a federal proceeding or investigation.[4] Even though the Act chiefly regulated accounting practices and corporate fraud, "prosecutors have since its enactment endeavored to expand its reach far beyond the corporate fraud context,"[5] applying Sarbanes-Oxley's provisions to a wide range of contexts, including child pornography,[6] narcotics,[7] and terrorism.[8]

Moreover, an increasing number of cases involving the obstruction of justice statutes—specifically, 18 U.S.C. §§ 1512(c) and 1519—involve the destruction or concealment of digital data: emails, files, and other electronically stored information ("ESI"). Despite

---

1. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (2002); *see also* Elisabeth Bumiller, *Bush Signs Bill Aimed at Fraud in Corporations*, N.Y. Times (July 31, 2002), http://www.nytimes.com/2002/07/31/business/corporate-conduct-the-president-bush-signs-bill-aimed-at-fraud-in-corporations.html.

2. 116 Stat. at 745.

3. 148 CONG. REC. S7350-04 (daily ed.July 25, 2002) (statement of Sen. Leahy).

4. 18 U.S.C. § 1512(c)(1) (2008); *accord* 18 U.S.C. § 1519 (202).

5. Sarah O'Rourke Schrup, *Obstruction of Justice: Unwarranted Expansion of 18 U.S.C. § 1512(c)(1)*, 102 J. CRIM. L. & CRIMINOLOGY 25, 26 (2012).

6. *See, e.g.,* United States v. McKibbins, 656 F.3d 707, 710 (7th Cir. 2011) (charging obstruction of justice under § 1512 because defendant attempted to destroy electronics containing child pornography).

7. *See, e.g.,* United States v. Johnson, 655 F.3d 594, 603-05 (7th Cir. 2011) (charging obstruction of justice under § 1512 because defendant destroyed drug contraband).

8. *See, e.g.,* Indictment at 15, United States v. Matanov, No. 1:14-CR-10159, 2014 U.S. Dist. Ct. Motions LEXIS 22893 (D. Mass. Aug. 11, 2014) (charging an associate of the Boston Marathon Bombers with obstruction of justice under § 1519 for deleting files and clearing browser history). Note that superseding information filed on Jan. 12, 2015 changed the charge to a violation of 18 U.S.C. § 1001(a)(1) (falsifying, concealing, or covering up a material fact in a federal investigation).

this, few cases have directly addressed whether a law primarily aimed at preventing the shredding of paper documents readily applies to ESI. Most courts have either ignored the issue or simply assumed that the statutes apply. The few courts that have dealt with the issue have not provided a comprehensive, forward-looking analysis of what acts constitute mutilation, destruction, or concealment of records, documents, or other objects.

This Note argues that the destruction or concealment of digital data constitutes obstruction of justice if the deletion or overwriting occurs manually, as opposed to automatically, and if the data is rendered inaccessible or unusable through that deletion or overwriting. Part II of this Note provides an overview of notable applications of the law, along with a discussion of the text and legislative history. Part III briefly highlights the challenges of defining the *actus reus* in light of recent technological changes. Finally, Part IV offers a number of possible solutions to this challenge and evaluates the advantages and shortcomings of each approach.

II. OVERVIEW OF 18 U.S.C. §§ 1512(C) AND 1519[9]

This section will begin with an overview of the relevant statutory language, followed by a brief overview of the "easy" cases, where courts presumed that Sarbanes-Oxley applied to the relevant conduct. It will then turn to the more challenging question of how the Act has been applied to electronically and digitally stored information, particularly in light of the Act's legislative history, before turning to cases that intensely grappled with the Act's scope, both in and out of the digital context.

Section 1102 of Sarbanes-Oxley added a new section to the pre-existing prohibition on witness and evidence tampering. The

---

9. Numerous other statutes have similar language to §§ 1512 and 1519, *see, e.g.*, 18 U.S.C. § 2232 (2000) ("Destruction or removal of property to prevent seizure."), but this Note will only examine the aforementioned obstruction of justice provisions. 18 U.S.C. § 1505 (2004), another obstruction of justice provision, also has similar language to §§ 1512 and 1519, but will not be discussed directly because the relevant language is relatively limited in its applicability. *See id.* § 1505 ("Whoever, with intent to avoid, evade, prevent, or obstruct compliance, in whole or in part, with any civil investigative demand duly and properly made under the Antitrust Civil Process Act, willfully withholds, misrepresents, removes from any place, conceals, covers up, destroys, mutilates, alters, or by other means falsifies any documentary material, answers to written interrogatories, or oral testimony, which is the subject of such demand; or attempts to do so or solicits another to do so . . . .").

addition, codified at 18 U.S.C. § 1512(c), closed a loophole that criminalized threatening or coercing someone into tampering with evidence, but did not prohibit evidence tampering itself.[10] As Senator Patrick Leahy explained, "section 1512(b) [made] it a crime to persuade another person to destroy documents, but not a crime for a person to destroy the same documents personally."[11]

The revised law reads

> Whoever corruptly—
>
> (1) alters, destroys, mutilates, or conceals a record, document, or other object, or attempts to do so, with the intent to impair the object's integrity or availability for use in an official proceeding; or
>
> (2) otherwise obstructs, influences, or impedes any official proceeding, or attempts to do so,
>
> shall be fined under this title or imprisoned not more than 20 years, or both.[12]

§ 1512(c) deals with a different type of conduct than the rest of the section: "it addresses interference with 'record[s], document[s], or other object[s],' while other subsections of § 1512 deal with persons."[13] In other words, "[t]he new crime reaches the conduct of an 'individual shredder' without the need to show that the defendant persuaded another to destroy or withhold documents."[14]

§ 1519 similarly addresses tampering with records and documents, as opposed to influencing other people. Passed as Section 802 of Sarbanes-Oxley, § 1519 reads:

> Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record,

---

10. *See* 18 U.S.C. § 1512(a); § 1512 (b); § 1512(c).

11. S. REP. NO. 107-146, at 6 (2002).

12. 18 U.S.C. § 1512(c) (2008).

13. Matthew Harrington et al., *Obstruction of Justice*, 52 AM. CRIM. L. REV. 1385, 1416 (2015). More specifically, § 1512(c) criminalizes threatening or coercing other *people* into engaging in document destruction, whereas § 1519 criminalized the act of destruction itself. This odd loophole exists because § 1512 was originally passed as a witness tampering statute. *See* § 1512 ("Tampering with a witness, victim, or an informant").

14. Beryl A. Howell & Andrew Weissman, *Obstruction for Data Destruction After Andersen*, 235 N.Y. L. J. NO. 110 (June 8, 2006).

> 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.[15]

Like § 1512(c), § 1519 criminalizes "alter[ing], destroy[ing], mutilat[ing], or conceal[ing]" records and documents, but further prohibits "cover[ing] up, falsif[ying], or mak[ing] a false entry," indicating that the provision criminalizes a broader range of conduct.[16] And, although the two sections have different *mens rea* requirements—"corruptly" in § 1512(c) and "knowingly" in § 1519—both sections require that the defendant actively obstruct a proceeding or investigation, instead of proscribing purely passive conduct.[17]

Since the passage of these two sections in 2002, hundreds of cases have been brought under §§ 1512(c) and 1519. Collectively, these cases provide, at best, a murky picture of what satisfies the *actus reus* requirement of destroying, mutilating, or concealing a record, document, or object. This section will highlight the commonalities and differences among applications of the obstruction of justice statutes.

A. Presumptively Reasonable Applications of Sarbanes-Oxley

In the majority of cases, courts do not articulate the precise definitions of "destroy," "mutilate," or "conceal;" defendants and courts alike often presume that the prosecutor's decision to charge

---

15. 18 U.S.C. § 1519 (2002).

16. *Id.*

17. *See United States v. Brown*, No. 14 CR 674, 2015 WL 6152224 at *4 (N.D. Ill. Oct. 19, 2015) (concluding that while § 1519 "only criminalizes the making of a false entry" and not an omission, an omission, such as a failure to check a box, can nonetheless constitute an affirmative act if it can be proved that a defendant knew that "failing to check a box represents that the conduct did not occur."); *cf.* United States v. Machi, 811 F.2d 991, 997-98 (7th Cir. 1987) (holding that the word "intentionally" in 18 U.S.C. § 1503, another obstruction of justice provision, modifies the *actus reus* requirement such that the defendant must act intentionally, as opposed to unconsciously); *but see* United States v. Gray, 692 F.3d 514, 517-18 (6th Cir. 2012) (noting that the failure to record the use of a restraint hold in subduing a detainee in a report constituted a "fabricated report"); United States v. Norman, 87 F. Supp. 3d 737, 743 (E.D. Pa. 2015) (discussing a number of cases that assume without discussion that § 1519 applies to omissions).

comports with the language of the statute, hence the minimal analysis as to whether the law actually proscribes the relevant conduct. Nevertheless, the prosecuted activity provides a useful baseline for determining what clearly qualifies as destruction, mutilation or concealment.[18] Specifically, the statutory language obviously encompasses severe physical destruction, and, in particular, reducing an object to pieces.

The more conventional of these cases, such as shredding paper shipment records[19] or tearing up and throwing out subpoenaed documents,[20] easily fall within the realm of destroying or mutilating a record. Even if these cases do not explicitly articulate the point, the shredding of paper documents represents the archetypal case contemplated by Sarbanes-Oxley. Multiple members of Congress specifically praised the Act for criminalizing shredding,[21] and Senator Leahy, an author and sponsor of the bill, primarily conceived of the law as an anti-shredding statute. [22] Other cases have taken a slightly broader view, but still hew closely to the general notion of shredding documents, such as placing records in a trash compactor. [23]

A number of other cases involve activities less clearly analogous to shredding, but nevertheless permit prosecutions to go forward without any meaningful discussion of the statutory text or legislative history to justify interpreting the Act broadly, suggesting that these actions fall within the plain meaning of the statute. For example, individuals have been prosecuted for obstruction of justice for physically breaking a circuit board apart;[24] prying open and damaging a hard drive;[25] lighting a cell phone, laptop, and other

---

18. A precise definition of "alter" will not be provided because "alter" likely refers to the contents of the document, and defining that term is not complicated by the transition from paper to electronic records.

19. *United States v. Richter*, 796 F.3d 1173, 1179 (10th Cir. 2015) (prosecuted under § 1519), *cert.* dismissed, Nov. 2016 U.S. LEXIS 2273 (2016), *and cert. denied*, 2016 U.S. LEXIS 3330 (2016).

20. *United States v. Jahedi*, 681 F. Supp. 2d 430, 433 (S.D.N.Y. 2009) (prosecuted under § 1512).

21. 148 CONG. REC. H5462-02 (daily ed. July 25, 2002) (statements of Representative Royce, a member of the Conference Committee, and Representatives Bereuter, Conyers, Roukema, Sensenbrenner and Tiahrt).

22. *See* 148 CONG. REC. S7350-04 (daily ed. July 25, 2002) (statement of Sen. Leahy). Senator Leahy authored the Corporate and Criminal Fraud Accountability Act, which later became Title VIII of Sarbanes-Oxley.

23. *United States v. Stover*, 499 F. App'x 267, 270 (4th Cir. 2012).

24. *United States v. Waterman*, 755 F.3d 171, 172 (3d Cir. 2014).

25. *Id.* at 173.

electronic equipment on fire;[26] taking apart a computer;[27] shooting a recording device;[28] and attempting to destroy a computer or hard drive by exposing it to water.[29] None of these acts perfectly correlate to shredding, but these courts uniformly agree that these acts qualify as destruction, mutilation, or concealment of a record, document, or object.

Neither the defendants nor the courts in these cases are likely to raise any objection to the charge that these acts qualify as obstruction of justice because they easily fit within the plain meaning of the statutory language. The precise definitions of the words used in the statutes—specifically "destroy" and "mutilate"—involve high degrees of physical impairment, akin to burning or smashing an item. Destruction and mutilation suggest that an object must be thoroughly damaged or otherwise rendered unusable or incomplete.[30] Because actions like setting fire to a laptop or physically pulling apart a computer easily fall within the conventional definitions of these terms, courts do not engage in rigorous statutory interpretation in these cases.

B. Applying Sarbanes-Oxley to Digitally and Electronically Stored Information

---

26. *United States v. Vrancea*, No. 12-CR-198, 2015 WL 5725883 at *1 (E.D.N.Y. Sept. 29, 2015), *appeal filed,* No. 15-3181(2d. Cir. Oct. 8, 2015).

27. *United States v. Russell*, 639 F. Supp. 2d 226 (D. Conn. 2007).

28. *United States v. Atkinson*, 532 F. App'x 873, 874 (11th Cir. 2013).

29. *United States v. Stanley*, 533 F. App'x 325, 329 (4th Cir. 2013) ("attempt[ing] to destroy [a] laptop by placing it under running water in the shower"); *United States v. Smyth*, 213 F. App'x 102, 104 (3d Cir. 2007) ("dump[ing] the actual hard drive in a body of water").

30. *See Destroy*, BLACK'S LAW DICTIONARY (10th ed. 2014) ("To damage (something) so thoroughly as to make unusable, unrepairable, or nonexistent; to ruin <destroying evidence>.") (first definition); *Mutilate*, BLACK'S LAW DICTIONARY (10th ed. 2014) ("To damage or change (something) so much that it is utterly spoiled; to render seriously defective by destroying or removing a material part of <the editors mutilated the essay beyond recognition>.") (second definition). In general, the term "conceal" similarly has a fairly conventional meaning. Concealment means "removing from sight or notice." *Concealment*, BLACK'S LAW DICTIONARY (10th ed. 2014) (second definition). Concealment can also mean "preventing disclosure or refraining from disclosing; esp., the injurious or intentional suppression or nondisclosure of facts that one is obliged to reveal." *Id.* (first definition). Given the 20-year penalty imposed by the obstruction of justice provisions and the severe character of the adjacent words, "destroy" and "mutilate," within the meaning of the statute, "conceal" probably carries a stronger connotation of "injurious or intentional suppression" as opposed to merely "refraining from disclosing." *Id.*

In another group of cases, courts have found sufficient evidence of obstruction of justice, even if the documents involved were not physically destroyed. These cases, like the ones discussed above, rarely contain thorough statutory interpretation. However, because the relevant activity usually occurs entirely on a computer, courts' failure to define how or why a particular act constitutes destruction, mutilation, or concealment suggests a presumption that the statute applies broadly—well beyond the paper shredding context. This presumption, though, rests on shaky ground, particularly in light of recent Supreme Court jurisprudence.[31]

The most common example of this group is the deletion of files from a computer or laptop.[32] Others involve the wiping[33] of devices, including iPods,[34] iPhones,[35] and desktop computers.[36] One of the earliest discussions of digital obstruction of justice occurred in *United States v. Kernell*.[37] Kernell deleted, in a number of different ways, information on his computer tied to the hacking of former Governor Sarah Palin's email account. He

> cleared the cache on his Internet Explorer browser, removing the record of websites he had visited during that period. He also uninstalled the Firefox internet browser,

---

31. *See infra* notes 42-50 and accompanying text.

32. *See, e.g.*, United States v. Davison, 492 F. App'x 391, 393 (4th Cir. 2012) (deleting images and videos stored on a blackberry and MP3 player); United States v. Keith, 440 F. App'x 503, 505 (7th Cir. 2011) (deleting video files); United States v. Ganier, 468 F.3d 920, 923 (6th Cir. 2006) (deleting files from various computers); United States v. Hollnagel, No. 10 CR 195, 2011 WL 3471081 at *1, *3 (N.D. Ill. 2011) (deleting data from a hard drive); *see also* United States v. Levine, 477 F.3d 596, 604 (8th Cir. 2007) (answering a jury question with the statement that deletion of files is obstruction of justice).

33. Although the precise definition of "wipe" may differ across sources, in general wiping a device erases everything, instead of one particular file, and renders all information previously on the device unusable. *See, e.g.*, *Data Wiping*, GARTNER (Jan. 16, 2016), http://www.gartner.com/it-glossary/data-wiping/; *Data Wiping Definitions*, W. MICH. UNIV. (Oct. 2011), http://www.wmich.edu/it/policiesdatawipedefinitions.

34. *United States v. Pugh*, No. 15-CR-116, 2015 WL 9450598 at *1 (E.D.N.Y. Dec. 21, 2015).

35. *United States v. Syed*, 616 F. App'x 973, 976 (11th Cir. 2015).

36. *United States v. Rappe*, 614 F.3d 332, 333 (7th Cir. 2010) ("[Defendant] had conversations with his girlfriend in which he told her to erase the information on the hard drives of the computers at their home in case federal law-enforcement agents arrived with a search warrant . . . . When a team of federal agents arrived and searched the apartment on March 19, 2007, the hard drives had been wiped clean, apparently with the aid of a computer program designed for this purpose.").

37. 667 F.3d 746 (6th Cir. 2012).

> which more thoroughly removed the record of his internet access using that browser, and ran the disk defragmentation program on his computer, which reorganizes and cleans up the existing space on a hard drive, and has the effect of removing many of the remnants of information or files that had been deleted. Finally, Kernell deleted a series of images that he had downloaded from the Palin email account.[38]

Likewise, several cases have involved the deletion of email or social media accounts, usually with the intention of erasing evidence of an online interaction or communication.[39] For example, one defendant attempted to delete a Google account that he had used for text messaging and Internet-based voice communication;[40] another defendant was charged with two counts of destruction of records under § 1519 for deleting his Gmail and Facebook accounts.[41]

All of these cases involving the destruction of online or digital data presume that Sarbanes-Oxley applies to electronically stored information and none of the opinions discuss whether or how a digital object can be destroyed or mutilated. This view is problematic in light of the Supreme Court's decision in *Yates v. United States*.[42] In *Yates*, the Court concluded that "'[t]angible object' in § 1519 . . . is better read to cover only objects one can use to record or preserve information, not all objects in the *physical* world."[43] The Court noted that, while "§ 1512(c)(1)'s reference to 'other object' includes any and every *physical* object,"[44] § 1519 has a narrower scope: "a 'tangible object' within § 1519's compass is one

---

38. *Id.* at 749.

39. *See, e.g.*, United States v. Gadsden, 616 F. App'x 539, 541-44 (4th Cir. 2015); *see also* United States v. Powell, No. 3:07-CR-324, 2013 WL 1165221 at *8 (E.D. Va. 2013) ("Powell asked Haghighi to 'store' his computer in the computer box in the closet on Haghighi's balcony, '[l]og in to my computer,' delete all email messages from Microsoft Outlook, and delete specific Google Gmail accounts, including '*EVERY* Google account you see on my computer on Internet Explorer'" in order to prevent police from finding evidence of a fraudulent Internet-based merchandise selling scheme) (modification and emphasis in original).

40. *Syed*, 616 F. App'x at 975-76.

41. United States v. Scott, No. 2:13CRL64, 2014 WL 2808802, at *1 (E.D. Va. 2014) (citing ECF No. 39, superseding indictment).

42. 135 S. Ct. 1074 (2015).

43. *Id.* at 1081 (plurality opinion) (emphasis added).

44. *Id.* at 1084 (emphasis added).

used to record or preserve information."[45] While this leaves open the possibility that "other object" in § 1512 applies to a much broader range of items, the Court still characterized both § 1512 and § 1519 as primarily applying to physical, not electronic, items.

Ultimately, though, the Court declined to rule on whether the term "tangible object" covers electronic or digital objects, such as emails or computer files. The plurality cited the Federal Sentencing Guidelines, which state that "'[r]ecords, documents, or tangible objects' includes (A) records, documents, or tangible objects that are stored on, or that are, magnetic, optical, digital, other electronic, or other storage mediums or devices; and (B) wire or electronic communications."[46] But the plurality only used this language to illustrate that "tangible object" refers to "objects used to record or preserve information," withholding comment on whether the phrase encompasses digital data.[47] The plurality likewise concluded that "computers, servers, and other media on which information is stored" qualify as tangible objects, but did not comment on whether the stored information itself fits within the statute's language.[48]

Justice Alito's concurrence addressed the issue directly, noting that the phrase "tangible objects" more readily applies to a hard drive than an email, but concluded nevertheless that "adding 'tangible object' to § 1519 would ensure beyond question that electronic files are included."[49] The dissent rejected this logic, arguing that Congress would have used the phrase "electronic communications," as opposed to "tangible objects," if it sought to cover emails and other electronic files.[50]

Despite restricting the application of § 1519 to objects used to store or record information, the Court's interpretation left untouched the prevailing view among circuit courts that Sarbanes-Oxley—and in particular § 1512—applies in many different contexts. For example, the Seventh Circuit concluded in *United States v. Johnson* that "[w]hen § 1512 was first enacted in 1982, it was not limited to the white-collar crime context," and therefore should apply in a wide

---

45. *Id.* at 1088-89.

46. U.S. SENTENCING GUIDELINES MANUAL § 2J1.2, comment., n.1 (2014).

47. *Yates*, 135 S. Ct. at 1085-86.

48. *Id.* at 1081.

49. *Id.* at 1089 (Alito, J., concurring) ("what is similar to a 'record' or 'document' but yet is not one? An e-mail . . . A hard drive, however, is tangible and can contain files . . . .").

50. *Id.* at 1100 (Kagan, J., dissenting)

variety of circumstances. [51] Based on the similar language throughout § 1512, the Seventh Circuit found that "alter, destroy, mutilate, or conceal" is not limited to instances of corporate fraud, or even to objects that contain information.[52] Other courts have similarly construed the statutory language broadly.[53] Since the Court's holding in *Yates* only ruled on the meaning of "tangible object" in § 1519, this broader interpretation of § 1512 still governs in most jurisdictions.

Based on this reasoning, courts have implicitly concluded that, because Sarbanes-Oxley applies to different types of crimes, it should also apply to all manner of cybercrime.[54] This assumption, however, lacks a strong grounding in the legislative history. The Senate Report, in discussing the need for new financial and corporate accounting regulations following the collapse of Enron and the related accounting scandal at Arthur Andersen,[55] noted that Arthur Andersen's "systematic destruction of records apparently

---

51. United States v. Johnson, 655 F.3d 594, 603 (7th Cir. 2011).

52. *Id.* at 604 (discussing cases that applied the phrase "other objects" to terms dissimilar from records and documents).

53. *See, e.g.,* United States v. Ortiz, 220 F. App'x 13, 17 (2d Cir. 2007) (applying § 1512(c)(1)'s "other object" language to a car*); United States v. Davis,* 531 F. App'x 601, 607 (6th Cir. 2013) (burning a car falls within the language of § 1512(c)(1)); United States v. Akiti, 701 F.3d 883, 887-88 (8th Cir. 2012) (destroying currency); United States v. Thompson, 237 F. App'x 575, 576 (11th Cir. 2007) (destroying a gun, money, and drugs).

54. *See, e.g.,* United States v. Katakis, 800 F.3d 1017, 1023 (9th Cir. 2015) (requiring government to prove destruction or concealment of 'electronic records and documents'); United States v. Kernell, 667 F.3d 746, 749 (6th Cir. 2012) (discussing an obstruction of justice charge brought for "clear[ing] the cache on his Internet Explorer browser, removing the record of websites [defendant] had visited during that period . . . uninstall[ing] the Firefox internet browser, which more thoroughly removed the record of his internet access using that browser, and [running] the disk defragmentation program on his computer . . . removing, many of the remnants of information or files that had been deleted."); United States v. Fumo, 504 F. Supp. 2d 6, 33 (E.D. Pa. 2007).

55. Enron was one of the largest companies in the United States until it rapidly collapsed and declared bankruptcy. Arthur Andersen was one of the largest auditing and accounting firms in the country, and served as Enron's accountant. Arthur Andersen engaged in improper accounting techniques that contributed to Enron's collapse. After the Securities and Exchange Commission announced that it was investigating Enron, a partner at Arthur Andersen ordered the destruction of thousands of records. Richard A. Oppel, Jr. & Kurt Eichenwald, *Enron's Collapse: The Overview; Arthur Andersen Fires an Executive for Enron Orders*, N.Y. TIMES (Jan. 16, 2002) http://www.nytimes.com/2002/01/16/business/enron-s-collapse-overview-arthur-andersen-fires-executive-for-enron-orders.html.

extended beyond paper records and included efforts to purge the computer hard drives and E-mail system of Enron related files."[56] However, beyond this statement, no indication exists in the record that either § 1512(c) or § 1519 served to address this problem. Instead, most discussion of the new criminal penalties included in Sarbanes-Oxley focuses on document shredding and eliminating loopholes in the prior statutory regime.[57]

As noted above, various members of the House of Representatives likewise indicated that the statute primarily applied to the shredding of paper documents. To the extent that other conduct was discussed at all, four congresspeople merely stated that the Act would apply to "other forms of obstruction of justice."[58] Senator Leahy similarly limited his description of the bill's scope to physical, as opposed to electronic or digital, evidence.[59] Conversely, in discussing § 1520,[60] which criminalizes the failure to preserve financial audit papers, Senator Leahy explicitly noted that the provision specifically includes "electronic communications, such as emails and other electronic records."[61] At the very least, these statements indicate that Congress primarily conceived of these sections as anti-shredding provisions, not more generalized

---

56. S. Rep. No. 107-146, at 4 (2002) (Senate Report on The Corporate and Criminal Fraud and Accountability Act of 2002, which was later added, in near identical form, to the Sarbanes-Oxley Act) (quotation marks omitted).

57. Looking at the legislative history of the phrase "alter, destroy, mutilate, or conceal," first introduced as part of the Victim and Witness Protection Act of 1982 ("VWPA"), likewise fails to provide any clear definitions. The VWPA, in creating § 1512, sought to protect "witnesses, victims, or informants" from intimidation by criminal defendants. S. Rep. No. 97-532, at 14 (1982). The precise meaning of the terms was not discussed by the Senate Report or in the floor debate, since the focus was on witness, not evidence, tampering.

58. *Id.* (statements of Representatives Bereuter, Roukema, Sensenbrenner, and Tiahrt).

59. Incidentally, this also suggests that § 1519's language referring to "tangible objects" only refers to physical objects, contrary to the view of the plurality in *Yates* and the vast majority of judicial circuits.

60. 18 U.S.C. § 1520(a)(2) (2015) ("The Securities and Exchange Commission shall promulgate . . . such rules and regulations, as are reasonably necessary, relating to the retention of relevant records such as workpapers, documents that form the basis of an audit or review, memoranda, correspondence, communications, other documents, and records (*including electronic records*) which are created, sent, or received in connection with an audit or review and contain conclusions, opinions, analyses, or financial data relating to such an audit or review, which is conducted by any accountant who conducts an audit of an issuer of securities . . . .") (emphasis added).

61. 148 Cong. Rec. S7418-01 (daily ed. July 26, 2002).

obstruction of justice provisions. Nevertheless, prosecutors have charged numerous individuals under Sarbanes-Oxley for deleting digital information.

The vast majority of cases that deal with digital obstruction of justice, then, incorrectly presume that the law applies broadly. Despite the relatively narrow purpose of the act as described in the legislative history, and the Supreme Court's narrow reading of the statutory language, most opinions do not try to define the scope of the Act or explain why it applies to so many different actions in so many different contexts.

C. Attempts to Define the Contours of the Actus Reus

A small number of decisions have engaged the question of how exactly the *actus reus* should be defined. Although these opinions generally favor a more expansive reading of the statutes, their reasoning and their conclusions differ in significant ways, ranging from the view that any act which contributes to obstruction is necessarily obstructive, to the notion that a proceeding or investigation must actually be obstructed to warrant prosecution.

In *United States v. Lessner*, the Third Circuit considered two different charges under § 1519: one for throwing an appointment book in the trash in front of two agents and another for calling an accomplice and asking him to remove a folder and destroy the contents.[62] As to the latter charge, the court concluded that because the accomplice ultimately "tore the contents into pieces" or, at the very least, concealed the folder by removing it from the defendant's desk and taking it to her car, the elements of the crime were satisfied.[63] The court's analysis similarly glossed over the more difficult question of whether throwing an appointment book into the trash constituted destruction of a record, cursorily concluding that "Lessner's act of disposal—which seems clearly to be a form of 'destruction'—falls within the proscriptions of the statute."[64] The court further argued that, because the agents did not know that the appointment book contained material information, "the disposal of the appointment book was also an attempt to conceal and cover up a record."[65]

The Third Circuit's reasoning in *Lessner* entails an incredibly broad view of the word "destroy." To conclude that placing an

62. 498 F.3d 185, 191 (3d Cir. 2007).

63. *Id.* at 191, 198.

64. *Id.* at 196, n.5.

65. *Id.* (quotation marks omitted).

appointment book in the trash constitutes destruction presumes that the trash can will be emptied and its contents disposed of. However, the actual disposal process may occur infrequently or involve several intermediaries before the contents are actually destroyed. The Third Circuit, then, appears to have adopted the view that participating in any step of the process that ultimately destroys the object satisfies the obstruction of justice statute. This view certainly encompasses placing records into a trash compactor,[66] but may actually go further: the trash compactor presumably would have destroyed the records had agents not recovered them first, but Lessner's deskside trash can probably did not function as an incinerator; several more steps would have had to be completed before objects thrown in the trash are actually destroyed. Nevertheless, the Third Circuit suggests that throwing something in the trash qualifies as destruction.

The *Lessner* court's reasoning relies, in part, on the assumption that Congress intended for § 1519 to apply broadly.[67] However, the Third Circuit misreads Senator Patrick Leahy's statements as to the breadth of the bill. Senator Leahy described § 1519 as correcting a flaw in the prior law; namely, he expressed concerns that the prior law "regarding destruction of evidence [was] full of ambiguities and technical limitations."[68] The new obstruction of justice provision was "meant to apply broadly to any acts to destroy or fabricate physical evidence."[69] But his primary concern was not that prior law failed to criminalize enough obstructive actions, but rather that the prior provisions "ma[d]e it a crime to persuade another person to destroy documents, but not to actually destroy the same documents yourself. Other provisions . . . have been narrowly interpreted by the courts . . . to apply only to situations where the obstruction of justice can be closely tied to a pending judicial proceeding."[70] Given this concern, Senator Leahy's statement that Sarbanes-Oxley is broader than the preceding statute only meant that the law should apply in cases where no specific proceeding is pending.[71] The Third Circuit read

---

66. *See* United States v. Stover, 499 F. App'x 267, 270 (4th Cir. 2012).

67. Lessner, 498 F.3d at 196, n.5. (citing 148 Cong. Rec. S7419 (daily ed. July 26, 2002) (statement of Sen. Leahy)).

68. 148 Cong. Rec. S7418-01 (daily ed. July 26, 2002) (statement of Sen. Leahy).

69. *Id.*

70. *Id.* (referencing United States v. Aguilar, 515 U.S. 593, 600 (1995) (holding that the obstruction of justice provision requires a "nexus" in time, causation, or logic between the act and the proceeding)).

71. *See* Dana E. Hill, Note, *Anticipatory Obstruction of Justice: Pre-emptive Document Destruction Under the Sarbanes-Oxley Anti-Shredding Statute, 18*

too much into Senator Leahy's statement about the statute's breadth, and failed to take into account the context of his comments.

The *Lessner* court's extraordinarily broad reading of the statute has reappeared throughout cases involving digital data. Cases involving the physical destruction of electronic storage devices, such as those discussed in Part II.A, do not expressly adopt the broad view articulated in *Lessner*, instead following a more conventional understanding of destruction. But courts have implicitly applied the term "destroy" and "conceal" to a wide range of conduct, particularly in cases that involve the deletion of digital files, like those discussed in Part II.B. As noted above, these cases rarely discuss precisely why the language of the statute applies.

The Fifth Circuit stands out as an exception in its attempts to demarcate the boundaries of the obstruction of justice statute, particularly in the digital context.[72] In *United States v. Simpson*, the court did not rule out the possibility that the "mere deletion of email" might fall within the conduct proscribed by § 1512(c)(1), but held that reformatting a drive in such a way as to make the data unusable—"as if the data had been 'splashed all over the drive'"—definitively did.[73] The court also noted that providing agents with only one hard drive when the device has been set up so that two drives had to be read together to properly access the stored information also qualified as obstruction.[74] The court suggested that making data "unusable" or, at the very least, "harder to recover" more accurately describes the scope of the statute.[75] While not a significant limitation on the scope of the statute, *Simpson* takes a marginally narrower approach than *Lessner*. Instead of including acts that might contribute to destruction or concealment at a later point in time, the Fifth Circuit indicated that the action actually has to make recovery more difficult.

The Ninth Circuit took a similar approach, but provided a more precise and comprehensive explanation of its reasoning. In *United States v. Katakis*, the Ninth Circuit concluded that "plac[ing] the emails into the deleted items folder . . . is not sufficient to satisfy

---

U.S.C. § 1519, 89 CORNELL L. REV. 1519, 1559 (2004) (concluding, based on the legislative history, that Senator Leahy only intended for prosecutors to be bound by an intent and a jurisdictional element, but not by a "pending proceeding" requirement).

72. *See* United States v. Simpson, 741 F.3d 539, 551-52 (5th Cir. 2014).

73. *Id.* at 551-52.

74. *Id.* at 552.

75. *Id.*

§ 1519."[76] The court reasoned that moving emails into a digital trash folder is not the same as placing a document in a physical trash can because

> a trash can is eventually emptied into a larger receptacle, the trash is mingled with other garbage, and the garbage is then either destroyed or placed in a location in which it is extremely difficult to find any particular item. On Katakis's computer, in contrast, an email placed in the deleted items folder remained in that folder unless a user took further action.[77]

In short, the court concluded that moving a document from its most obvious location does not qualify as actual obstruction.[78] The court ultimately held that, to qualify as obstruction, an action must actually diminish the likelihood that that a file will be found or recovered.[79]

Broadly speaking, then, there have been two explicitly articulated views of the scope of the obstruction of justice statute. The first suggests an expansive reading, including steps that contribute to obstruction. The second offers a marginally narrower reading and requires that an action actually make it more difficult to recover the information contained in the relevant record or document. However, neither approach has been widely adopted and most courts remain content to permit broad application of Sarbanes-Oxley without determining whether the Act actually proscribes the conduct at issue.

III. THE NEED FOR CLARITY IN THE OBSTRUCTION OF JUSTICE STATUTES

The preceding cases illustrate just how broadly prosecutors and courts have applied §§ 1512 and 1519. An incredible range of activities have been treated as obstruction of justice, including encryption, clearing browser history, deleting emails, wiping hard

---

76. United States v. Katakis, 800 F.3d 1017, 1029 (9th Cir. 2015).

77. *Id.*

78. *Id.* at 1030.

79. *Id.* at 1029. The Sixth Circuit entertained a similar argument in permitting an expert to testify "that the files in question were transferred to the recycle bin rather than deleted." United States v. Ganier, 468 F.3d 920, 923 (6th Cir. 2006). The court did not rule on whether the movement of those emails actually satisfies the *actus reus* requirement, but indicated that such an argument warranted testimony and argument.

drives, and deleting social media accounts. And yet few courts have rigorously considered which activities fall within the purview of the statute and why. As an increasing amount of information is sent and stored digitally, this opens up the possibility for a wide range of prosecutions or additional charges. For example, several people have suggested that Hillary Clinton could be prosecuted for obstruction of justice under 18 U.S.C. § 1519, but these claims usually presume that the deletion of even one email constitutes obstruction of justice. [80]

In less politically charged circumstances, the applicability of the obstruction of justice statutes still matters, especially for corporate enterprises that have extensive document retention policies. "Many corporations utilize 'disk-wiping' technology, which protects deleted documents from later retrieval" as part of their general document retention policy.[81] Misuse of this technology, however, "can lead to penalties in both civil and criminal cases."[82] Even though many programs automatically delete electronically stored information after a certain period of time in compliance with a retention policy, courts increasingly "attach the obligation to preserve documents [in civil cases] earlier than the filing of a complaint—as soon as the party has knowledge that the information may be relevant to a potential claim,"[83] mirroring the temporal requirements of § 1519.[84] Not only

---

80. *See, e.g.*, Ronald D. Rotunda, *Hillary's Emails and the Law*, WALL ST. J., March 16, 2015, http://www.wsj.com/articles/ronald-d-rotunda-hillarys-emails-and-the-law-1426547356; *Judge Nap: 'Hillary Clinton Has Admitted to Destroying Evidence'*, FOX NEWS, March 30, 2015, http://insider.foxnews.com/2015/03/30/judge-napolitano-hillary-clinton-has-admitted-obstruction-justice.

81. Gary G. Grindler & Jason A. Jones, *Please Step Away from the Shredder and the "Delete" Key: §§ 802 and 1102 of the Sarbanes-Oxley Act*, 41 AM. CRIM. L. REV. 67, 91 n.125 (2004).

82. Christopher R. Chase, *To Shred or Not to Shred: Document Retention Policies and Federal Obstruction of Justice Statutes*, 8 FORDHAM J. CORP. & FIN. L. 721, 722 (2003).

83. Mary Kay Brown & Paul D. Weiner, *Digital Dangers: A Primer on Electronic Evidence in the Wake of Enron*, 30 No. 1 LITIGATION 24, 25(2003) (discussing numerous cases that indicate this trend).

84. § 1519 proscribes any conduct "in relation to or contemplation of" any proceeding, a phrase which courts have interpreted to mean any proceeding, even one that has not started or that the defendant is unaware of. *See* United States v. Yielding, 657 F.3d 688, 711 (8th Cir. 2011) ("The statute . . . does not allow a defendant to escape liability for shredding documents with intent to obstruct a foreseeable investigation of a matter within the jurisdiction of a federal agency just because the investigation has not yet commenced."); *see also* Chase, *supra* note

is there significant overlap between civil and criminal liability, then, but the same action can lead to adverse outcomes in both contexts.[85] Because courts have concluded that the requisite intent for obstruction of justice can be formed even if an investigation or proceeding is only foreseeable,[86] the Act may apply to an extraordinary range of activities, including obstruction of a purely internal investigation[87] or civil litigation. Even relatively mundane actions, such as clearing an inbox or using a private browsing mode,[88] may qualify as obstruction of justice if done in contemplation of a federal investigation.

This raises a number of challenging but important questions that courts, legislators, and commentators have failed to fully examine. One critical but unaddressed issue is whether a basic setting on a computer, such as encrypting files or emails automatically or using private browsing as a default, qualifies as obstruction of justice if an individual does not alter the default settings once an investigation becomes foreseeable. Many of these issues have already arisen in the civil context with spoliation of evidence,[89] but they have not yet been fully addressed in the criminal context.

82, at 743 ("the timing of the act in relation to the beginning of the matter or investigation is also not a bar to prosecution.") (citations omitted).

85. *Cf.* Superseding Indictment, United States v. Kolon Indus., Inc., No. 3:12-CR-137, 2013 WL 1178216 (E.D. Va. March 19, 2013) (charging various individuals with obstruction of justice for deleting files related to a civil suit).

86. *Yielding*, 657 F.3d at 711.

87. *See* Michael M. Farhang, *Section 1519: Why Obstructing an Investigation by Company Counsel May Now Be a Federal Crime*, 4 WCR 191, 195-96 (Mar. 13, 2009) (discussing an obstruction of justice prosecution based on false statements made to company's counsel during an internal investigation with no pending federal investigation).

88. Private browsing mode automatically deletes temporary internet files, such as cookies, and clears the browser's history at the end of the session. All major browsers have some form of private browsing mode. *See, e.g.*, *InPrivate Browsing*, MICROSOFT http://windows.microsoft.com/en-US/internet-explorer/products/ie-9/features/in-private (last visited Jan. 21, 2016, 8:38 PM); *Browse in private with incognito mode*, GOOGLE, https://support.google.com/chrome/answer/95464?hl=en (last visited Jan. 21, 2016, 8:39 PM).

89. *See* Margaret M. Koesel & Tracey L. Turnbull, *Chapter 1: The Duty to Preserve Evidence*, SPOLIATION OF EVIDENCE: SANCTIONS AND REMEDIES FOR DESTRUCTION OF EVIDENCE IN CIVIL LITIGATION (Daniel F. Gourash, 3d ed. 2013) ("Many computer systems have automatic deletion features that periodically purge electronic documents, so once the duty to preserve is triggered, a party must also take active steps to halt any automatic deletion process.").

Moreover, the boundaries of the *actus reus*—destroying, mutilating, or concealing an object—remain undefined. As the Ninth Circuit noted in *Katakis*, the statute may not proscribe some activities, such as moving an email to the trash folder, because they may not sufficiently obstruct justice. In light of increasing use of email and digital storage of information, terms like destruction and concealment need more precise contours. To say that a person "destroyed" or "mutilated" an email sounds odd to the modern ear, and yet prosecutors have charged this precise crime.[90] Likewise, judges have encountered difficulties in analogizing between the destruction of tangible paper records and digital computer files.[91] Defining the *actus reus* of §§ 1512 and 1519, then, is critical to preventing possible abuses using this expansive law.

IV. DEFINING THE SCOPE OF §§ 1512 AND 1519

There are a number of possible ways of reading the terms of the obstruction of justice statutes. This Note will consider

1. the "broad" reading, which applies the statutes to essentially any activity that makes a document or record less accessible in any way;
2. the "actual obstruction" approach, which requires courts to determine the extent to which an act actually obstructed an investigation or proceeding; and
3. the "spoliation" approach, which attempts to import the civil rules governing preservation of evidence into the criminal context.

---

90. *See, e.g.*, United States v. Fumo, 628 F. Supp. 2d 573, 595 (E.D. Pa. 2007) ("conspired to destroy, aided and abetted in the destruction of, and did destroy e-mail and other electronic evidence").

91. *Cf.* David Axelrod et al., *Hard Times with Hard Drives: Paperless Evidence Issues That Can't Be Papered Over*, 25 CHAMPION 18, 23 (2001) (The authors note that, in deciding a motion to quash a subpoena for data stored on hard drives and floppy disks, one court observed that, "traditionally, 'subpoenas properly are interpreted as seeking categories of paper documents[,] not categories of filing cabinets,' and that such reasoning applies with even greater force to computer records, which may be efficiently selected through a key word search . . . The opinion highlights the difficulty of applying old law to new technologies. For instance, applying its 'filing cabinet' analogy, the court ordered the corporation to preserve intact 'the computer and related materials that were subjects of the quashed subpoena.' Preserving all such materials 'intact' might require suspending the use of the computer and installing substitute machines.") (footnotes omitted) (second alteration in original).

This section will examine the benefits and disadvantages of each before proposing an alternative that aims to address the shortcomings of the above approaches.

D. "Broad" Reading

The "broad" reading of the obstruction of justice statute has been adopted implicitly by several courts. This interpretation of the statute construes "alters, destroys, mutilates, or conceals" in the broadest possible fashion, particularly when considering prosecutions for the deletion of digital data. Prosecutions in this category have charged people with obstruction of justice for a wide range of conduct: deleting emails,[92] deleting files,[93] clearing browser history,[94] or using encryption.[95] Notably, these cases rarely discuss why an act qualifies as obstruction of justice, and usually assume that the mere act of deletion, [96] even if the document is easily recoverable,[97] satisfies the

---

92. *See* Superseding Indictment at 8, United States v. Ayache, 2014 WL 2881578 (M.D. Tenn. June 25, 2014) (No. 3:13-CR-153); *see also Fumo*, 628 F. Supp. 2d at 595; *In re: Grand Jury Investigation, No. 06–1474*, 445 F.3d 266, 275 (3d Cir. 2006) ("Jane Doe was committing the crime of obstruction of justice by participating in a scheme to delete emails on the computers of the Organization, its officers, and staff.").

93. United States v. Levine, 477 F.3d 596, 604 (8th Cir. 2007).

94. United States v. Kernell, 667 F.3d 746, 749 (6th Cir. 2012).

95. *See* William A. Hodkowski, *The Future of Internet Security: How New Technologies Will Shape the Internet and Affect the Law*, 13 Santa Clara Computer & High Tech. L.J. 217, 271 (1997) (noting that, even before Sarbanes-Oxley, the existing obstruction of justice provisions likely applied to encryption as a form of concealment).

96. For a simplified overview of how saving and deleting files works, *see* Axelrod, *supra* note 91, at 19-21 (defining various computer terms and explaining that "files may remain in a computer long after being deleted. Deleting a computer file does not erase it, but merely changes its 'address' in the computer storage device. Consequently, the file becomes invisible in standard applications. When a file is saved to a disk, for example, its address is saved in the [file allocation table]. 'Deleting' that file merely instructs the [file allocation table] to remove the file's name reference, but does not remove the file itself. That file may be out of sight and out of mind, but it is not out of reach until it is overwritten in its entirety. There is much discussion in the technical community regarding this point. Even overwriting may not delete a file.") (emphasis omitted).

97. *See* Darrin J. Behr, *Anti-Forensics: What It Is, What It Does and Why You Need to Know*, N.J. LAW., Dec. 2008, at 10 ("While some users may still be under the assumption that deleting files and sending them to the recycle bin results in rendering those documents irretrievable, this is not necessarily the case.").

law's *actus reus* requirement.[98] Moreover, courts rarely try to delineate the difference between attempted and completed obstruction; rather, discussions of the statute usually suggest that even relatively unobstructive acts still qualify as obstruction, regardless of whether or not additional steps must be taken to actually destroy the object.[99] In other words, this broad view of obstruction is not designed to punish only those who seek to destroy an object more fully, but instead seeks to encompass even incremental steps in the overall scheme.[100]

A broad understanding of the statute has certain advantages. When it comes to digitally stored files, "electronic storage costs are low" relative to storing paper documents, so encouraging companies and people to retain emails and files indefinitely does not impose a significant burden while still guaranteeing that law enforcement can obtain documents if necessary.[101] Moreover, this approach makes cases fairly easy for judges to decide: anything that in any way impairs access to or obfuscates the location of a file qualifies as obstruction of justice. This obviates the need for any fine-grained analysis of where to draw the line between innocent acts and criminal ones, since it would cover nearly all conduct.

This approach also represents one interpretation of Congress's purpose in passing the Sarbanes-Oxley Act. Although the legislative history does not specifically identify preventing the destruction of ESI as a purpose of the Act, the Enron/Arthur Andersen scandal that prompted the Act's passage involved the deletion of documents and emails from Arthur Andersen's files.[102] As such, limiting law enforcement's ability to prosecute for such acts may run counter to the purpose of the statute.[103] Finally, and perhaps most significantly, this would permit for an incredibly flexible analysis that is not tied

---

98. *Cf.* United States v. Lessner, 498 F.3d 185, 196 n. 5 (3d Cir. 2007) ("Lessner's act of disposal-which seems clearly to be a form of "destruction"-falls within the proscriptions of the statute.").

99. *See id.* at 206 (upholding a conviction for obstruction of justice for placing an appointment book in a garbage can); *see also* United States v. Stover, 499 F. Appx 267, 270 (4th Cir. 2012) (upholding an obstruction of justice conviction for placing documents in a trash compactor dumpster that were recovered prior to destruction).

100. *See* United States v. Lessner, 498 F.3d 185 (3d Cir. 2007).

101. Julia Schiller, *Deterring Obstruction of Justice Efficiently: The Impact of Arthur Andersen and the Sarbanes-Oxley Act*, 63 N.Y.U. ANN. SURVEY AM. L. 267, 284 (2007).

102. Indictment at ¶ 10, United States v. Arthur Andersen, 2002 WL 32153945 (S.D. Tex. Mar. 14, 2002) (Cr. No. CRH-02-121).

103. *See* Grindler, *supra* note 81, at 77.

to technological development, so courts would not have to worry about ever-evolving technology rendering their previous decisions untenable or inapplicable.

Despite these advantages, a broad reading would also carry significant negative consequences. Some commentators have already noted that Sarbanes-Oxley dramatically expanded the Government's ability to prosecute crimes in a wide range of areas[104] while others have noted that the penalties imposed by Sarbanes-Oxley may "overcriminalize" white collar crime.[105] Applying the statute to an overly broad range of conduct will likely raise many of the same problems: defendants may be "encourage[d] . . . to store haystacks"[106] of information because any deletion may run afoul of the statute. Such a broad reading may not "operate efficiently" because defendants may be "afraid to destroy documents in the normal course of business," raising overhead costs through unnecessary expenditures on data storage.[107]

Despite solving the line-drawing problem, bringing a wide range of conduct within the sweep of the statute may impose a disproportionate sentence on relatively innocuous activity, a result that Congress likely did not intend. For example, under a broad reading of the term "conceal," moving a document containing incriminating evidence from one digital folder to another may constitute obstruction of justice, even if both folders may be easily accessed.[108] By way of comparison, this would be the equivalent of criminalizing moving a record from one drawer in a filing cabinet to another. Imposing a twenty-year sentence for obstruction of justice for such an act seems inappropriate.[109] Even with the requisite *mens rea*, such an action only marginally obstructs an investigation or

---

104. *See* Schrup, *supra* note 5, at 25-26.

105. *See* Lucian E. Dervan, *White Collar Overcriminalization: Deterrence, Plea Bargaining, and the Loss of Innocence*, 101 KY. L.J. 723, 723-25 (2013).

106. Schiller *supra,* note 101, at 268.

107. *Id.*

108. Other examples of innocent conduct that may be caught up in a broad reading of the statute include deleting an email or file but leaving it in the trash folder indefinitely, or updating an internet browser but failing to import the history and bookmarks from the prior version.

109. *Cf.* United States v. Katakis, 800 F.3d 1017, 1029-30 (9th Cir. 2015) ("The Government's approach would all but eliminate the act requirement from the statute: so much as taking an incriminating document from the surface of a desk and placing it in a drawer, or putting another folder on top of it, would expose a defendant to a twenty-year prison sentence, so long as the defendant acted with even the faintest hope that investigators might overlook the document.").

proceeding. Given the severity of the penalty imposed,[110] applying the act to relatively innocent conduct likely violates the principle of proportionality.[111] If Congress sought to criminalize the mere shuffling of files around, it likely either would have made that explicit in the statutory text or the legislative history. In short, the broad reading brings too much innocent conduct within the purview of the statute, raising both proportionality and overcriminalization concerns, and therefore should be rejected.[112]

E. "Actual Obstruction" – The Katakis Approach

The Ninth Circuit explicitly articulated a more limited approach in *United States v. Katakis*.[113] In *Katakis*, the court concluded that "the Government must show actual obstruction."[114] While still fairly broad, this approach has the potential to curtail the scope of the obstruction of justice statutes.

Katakis arose "from an investigation by federal authorities into a scheme to rig bids at foreclosure auctions."[115] Katakis, upon learning that prosecutors had subpoenaed his bank records, "installed a program called DriveScrubber 3," which "is a program designed to wipe hard drives clean of all information" by "overwrit[ing] all of the information in a hard drive's unallocated or 'free' space."[116] Katakis proceeded to install the DriveScrubber program on four different computers, including two laptops that belonged to Swanger, an alleged co-conspirator.[117] On one of Swanger's computers, Katakis

---

110. §§ 1512(c) and 1519 impose a 20-year maximum sentence for obstruction of justice.

111. *See generally* Kristin Kenny, *The Sarbanes-Oxley Act: Balancing the Rights of Investors and the Rights of Corporate Officers*, 13 TEMP. POL. & CIV. RTS. L. REV. 151 (2003) (discussing possible Eighth Amendment and proportionality issues with Sarbanes-Oxley).

112. One partial solution to this problem would be to read the *actus reus* of §§ 1512 and 1519 broadly, but to construe the term "object" narrowly, to only apply to physical items. This reading may be a plausible extension of the Supreme Court's reasoning in Yates v. United States, 135 S.Ct. 1074 (2015), but would not accord with the history of the Act, given that Congress sought to target the actions of Arthur Andersen employees to shredded documents *and* deleted emails. Moreover, doing so fails to address the proportionality concerns of twenty-year sentences for merely placing an item into a deskside waste bin, as the United States v. Lessner, 498 F.3d 185 196 (3d Cir. 2007) court suggests.

113. 800 F.3d 1017.

114. *Id.* at 1030.

115. *Id.* at 1020.

116. *Id.*

117. *Id.*

deleted nearly 4,000 emails, including some emails sent between Swanger and Katakis.[118] After seizing the computers, "the Government discovered ten incriminating emails that implicated Katakis . . . in the deleted items folder in Swanger's email client."[119] Katakis was indicted for "delet[ing] and caus[ing] others to delete electronic records and documents" and for "install[ing] and us[ing] . . . a software program that overwrote deleted electronic records and documents so that they could not be viewed or recovered" in violation of § 1519.[120] Due to the collapse of its primary theory,[121] the Government ultimately argued at trial that, by hitting the delete key and sending the emails to the deleted items folder, Katakis had obstructed justice.[122]

In evaluating the Government's argument on appeal, the Ninth Circuit concluded that "moving . . . emails from the inbox to the deleted items folder" is not a sufficient "degree of concealment . . .

---

118. *Id.* at 1020-21.

119. *Id.* at 1021.

120. *Id.* The court also noted that, because the indictment failed to charge attempt, the Government had to prove actual deletion. Although this charging error likely informed the outcome of the case and the court's ultimate decision, the court's reasoning applies more generally to the definition of "concealment" or "destruction," whether or not the act is attempted to completed.

121. *Id.* at 1021-22 ("The Government proceeded to trial on the theory that Katakis ran the DriveScrubber program on his Dell, Swanger's ASUS, and the GD Mail Server to erase all traces of the ten incriminating emails. The Government's key witness was Medlin, who testified as an expert. Medlin testified that Katakis 'double-deleted' emails; that is, he deleted them once from the mail client and then again when he emptied the deleted items folder. After they were double deleted, the emails fell into the free space, where . . . they were . . . overwritten by DriveScrubber. Katakis called Don Vilfer as a rebuttal expert. Vilfer testified that Medlin's theory of what happened to double-deleted emails was incorrect . . . According to Vilfer, a double-deleted email would not fall into the free space . . . but would remain within the portion of the hard drive allocated for the Exchange database. The crux of Vilfer's testimony was that, given how the Exchange program operated, it would be impossible for DriveScrubber to overwrite any double-deleted emails, including the ten incriminating emails that were at the heart of the Government's case . . . Vilfer testified that he was able to recover thousands of double-deleted emails, but he could not find the ten incriminating emails. Vilfer agreed with Medlin that it was suspicious that there were no traces of the ten incriminating emails on any computer other than Swanger's Dell. However, he explained that absence by opining that the ten incriminating emails (including metadata) had been fabricated . . . In rebuttal, Medlin admitted that Vilfer's testimony was correct: it was impossible for DriveScrubber to have deleted the ten incriminating emails.").

122. *Id.* at 1022.

to satisfy § 1519," [123] even with the requisite *mens rea*.[124] The court reasoned that because "'[c]onceal is not a term of art . . . we are obligated to give the term its plain meaning."[125] The court rejected the notion that "conceal" means "remov[ing] something from its 'ordinary place of storage' making the thing 'more difficult to find.'"[126] Because "the first place that any competent investigator would look for emails that are not in the inbox is in the deleted items folder," such activity does not qualify as concealment within the meaning of § 1519.[127]

Ultimately, the Ninth Circuit declined to "set out a comprehensive standard for what it means to 'conceal' a record."[128] Nonetheless, the court noted that trial courts should consider "the effort that an investigator would have to expend to uncover a hidden document."[129] Therefore, concealment requires that "there must be some likelihood that the item will not be found."[130] However, the court explicitly limited its holding, noting that the emails left in the trash folder of Katakis's email client would remain there until a user took further action, as opposed to a physical trash can, where, presumably, "the trash is mingled with other garbage and the garbage is then either destroyed or placed in a location in which it is extremely difficult to find any particular item."[131]

The Ninth Circuit's approach has several attractive features: the language appears to be flexible and technology-neutral[132] in the

---

123. *Id.* at 1028-29.

124. *Id.* at 1030 ("Intent for an item not to be found is inherent in the act of concealment. If that intent is satisfied, there is almost no act with respect to a document that would not be criminal under the Government's proposed test.").

125. *Id.* at 1028 (defining conceal as ""to prevent disclosure or recognition of; avoid revelation of; refrain from revealing recognition of; draw attention from; treat so as to be unnoticed; to place out of sight; withdraw from being observed; shield from vision or notice.") (citing WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY (1993)).

126. *Id.*

127. *Id.* at 1029.

128. *Id.* at 1030.

129. *Id.*

130. *Id.*

131. *Id.* at 1029.

132. *Cf.* Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1007 (2010) ("Technology neutrality assumes that the degree of privacy the Fourth Amendment extends to the Internet should try to match the degree of privacy protection that the Fourth Amendment provides in the physical world. That is, courts should try to apply the Fourth

sense that it may be applied to a wide variety of programs or activities on different media. Moreover, it permits for a fairly simple analysis, since it primarily requires determining whether a particular action has any possibility of rendering a record or document "unfindable." Another advantage, at least from a prosecutor's perspective, is that it seems to cover a rather broad range of conduct and only excludes the most minimal types of obstruction. By its own admission, the Ninth Circuit recognized that it imposed a "low bar,"[133] and suggested that this approach not only accorded with a broad reading of the statutory language and legislative history, but also would not significantly impede the Government's ability to prosecute different types of obstruction.

However, this approach also has several issues that make it difficult to apply broadly. Although the approach is technology-neutral in that it applies to many different media, the language used by the court suggests that, as forensic tools improve, certain activities may fall out of the statute's scope because a concealed or partially destroyed document will always be found. Admittedly, the court indicated that, if forensic tools are necessary to find the document, then whatever action was taken qualifies as obstruction. But this does not square with the "likelihood of not being found" language in the opinion, since, with near-perfect recovery tools, a deleted document can almost always be found.

Moreover, rationale employed by the *Katakis* court raises a significant issue in that it makes the definition of obstruction turn more on the ability of an investigator to discover or recover a document than on the actions of the defendant. This could lead to disparate outcomes for defendants who engaged in the same conduct, but obstructed investigations of relatively tech-savvy government organs. Not only does this raise concerns regarding equality and fairness, but it also raises notice concerns: defendants likely do not know how capable federal investigators are when they begin deleting information of their computers, meaning that they cannot know ahead of time whether their actions will "actually obstruct" an investigation.

Therefore, while the *Katakis* approach more effectively draws a bright-line than the broad approach, it fails to address numerous issues that may plague future cases. Most significantly, *Katakis* shifts

---

Amendment in the new environment in ways that roughly replicate the role of the Fourth Amendment in the traditional physical setting.").

133. *Katakis*, 800 F.3d at 1030.

the relevant inquiry away from the actions of the defendant to the actions of the investigators.

F. "Spoliation" Approach

Another alternative involves importing discovery and spoliation concepts from the civil litigation context. This section will examine various attempts to categorize and structure spoliation rules, and then evaluate the applicability of such an approach to the criminal context. This section will begin by examining the "accessibility/inaccessibility" distinction that characterizes analyses of spoliation of digital data, and then consider how the legal community has dealt with the issue of automatic deletion.

Although no court has adopted this approach, the civil, as opposed to criminal, discovery rules provide a useful starting point for considering what constitutes obstruction of justice because the law surrounding civil discovery rules is fairly well-developed.[134] Moreover, many of the criminal rules dealing with digital data address the prosecutor's obligation to store and disclose data, not the defendant's.[135] Conversely, the penalties imposed by §§ 1512 and 1519 closely reflect the preservation requirements imposed on civil litigants.[136] Perhaps the best indicator that civil litigation practices may inform the scope of the obstruction of justice statutes

---

134. *See* Andrew D. Goldsmith, *Trends – Or Lack Thereof – In Criminal E-Discovery: A Pragmatic Survey of Recent Case Law*, 59 UNITED STATES ATTORNEYS' BULLETIN, 2 ("While civil litigators have grappled with discovery of ESI for years—for example, discovery of ESI was explicitly incorporated into the Federal Rules of Civil Procedure in December 2006—criminal law has lagged behind . . . a coherent body of case law on appropriate collection, management, and disclosure of ESI has yet to emerge in the criminal context.").

135. *See id.* at 4 ("Unlike civil litigation, which requires broad discovery on the basis of relevance, the prosecution's disclosure obligations are limited in scope, extending only as far as the requirements of *Brady* [*v. Maryland*], *Giglio* [*v. United States*], Jencks [Act, 18 U.S.C. § 3500], and [Federal Rule of Criminal Procedure] 16; that is, to material exculpatory and impeachment information; witness statements; a defendant's statements and prior record; certain documents, objects, and scientific reports; and expert witness summaries.").

136. *See* Justin P. Murphy and Louisa K. Marion, *E-Discovery in Government Investigations and Criminal Litigation*, THE STATE OF CRIMINAL JUSTICE, 2014, at 135 ("In civil litigation, the basic rule is fairly well-developed: 'Whenever litigation is reasonably anticipated, threatened or pending against an organization, that organization has a duty to preserve relevant information.' In general the same principle applies to the criminal arena: The duty to preserve potentially relevant information arises when a government investigation is contemplated, threatened, pending, or can be reasonably anticipated.") (footnotes omitted).

is that the Department of Justice has prosecuted companies and individuals for obstruction of justice based on activities that occurred in a civil suit.[137] Spoliation[138] can give rise to obstruction of justice or other criminal charges.[139] Nevertheless, translating principles from the civil context to the criminal poses numerous challenges because "different courts have decided similar e-discovery issues in very different ways,"[140] making it difficult to pull out precise trends. However, two components of spoliation stand out as applicable to obstruction of justice: accessibility and automation.

1. Accessibility/Inaccessibility

Some commentators and courts have discussed the challenges created by spoliation and document retention in terms of the difficulty of recovering or accessing the relevant information. One of the more comprehensive court decisions discussing the issue is *Zubulake v. UBS Warburg*.[141] In *Zubulake*, a gender-discrimination case, the court laid out different types of electronic data, concluding that the five major categories of data, in order of accessibility, are:

---

137. *See id.* at 137; *see also* United States v. Kolon Indus., Inc., 926 F. Supp. 2d 794, 797 (E.D. Va. 2013); *United States v. Lundwall*, 1 F. Supp. 2d 249, 255 (S.D.N.Y. 1998) (permitting obstruction of justice charges under § 1503 for destroying documents sought in a civil proceeding); *but see* Richmark Corp. v. Timber Falling Consultants, Inc., 730 F. Supp. 1525, 1532 (D. Or. 1990) (declining to apply § 1503 to a civil discovery dispute absent a court order or subpoena because of "the extensive framework of rules and remedies provided for the resolution of civil discovery disputes.").

138. The definition of spoliation even mirrors the obstruction of justice statute: "[t]he intentional destruction, mutilation, alteration, or concealment of evidence, usu[ally] a document." *Spoliation*, BLACK'S LAW DICTIONARY (10th ed. 2014).

139. Beryl A. Howell, *The Slippery Slope from Spoliation to Obstruction*, N.Y. L. J., July 27, 2006, at no. 16.

140. Justin P. Murphy, *E-Discovery in Criminal Matters – Emerging Trends & the Influence of Civil Litigation Principles Post-Indictment E-Discovery Jurisprudence*, 11 SEDONA CONF. J. 257, 257 (2010).

141. Zubulake v. UBS Warburg, LLC, 217 F.R.D. 309 (S.D.N.Y. 2003).

(1) active, online data;[142] (2) near-line data;[143] (3) offline storage/archives;[144] (4) backup tapes;[145] and (5) erased, fragmented or damaged data.[146] The court then drew a line between types 1, 2,

---

142. *Id.* at 318 ("*Active, online data*: 'On-line storage is generally provided by magnetic disk. It is used in the very active stages of an electronic records [sic] life—when it is being created or received and processed, as well as when the access frequency is high and the required speed of access is very fast, i.e., milliseconds.' Examples of online data include hard drives." (quoting Cohasset Associates, Inc., *White Paper: Trustworthy Storage and Management of Electronic Records: The Role of Optical Storage Technology* 10 (April 2003) ("White Paper")).

143. *Id.* at 318-19 ("*Near-line data*: 'This typically consists of a robotic storage device (robotic library) that houses removable media, uses robotic arms to access the media, and uses multiple read/write devices to store and retrieve records. Access speeds can range from as low as milliseconds if the media is already in a read device, up to 10 –30 seconds for optical disk technology, and between 20 – 120 seconds for sequentially searched media, such as magnetic tape.' Examples include optical disks." (quoting Cohasset Associates, Inc., *White Paper: Trustworthy Storage and Management of Electronic Records: The Role of Optical Storage Technology* 11 (April 2003) ("White Paper")).

144. *Id.* at 319 ("*Offline storage/archives*: 'This is removable optical disk or magnetic tape media, which can be labeled and stored in a shelf or rack. Off-line storage of electronic records is traditionally used for making disaster copies of records and also for records considered "archival" in that their likelihood of retrieval is minimal. Accessibility to off-line media involves manual intervention and is much slower than on-line or near-line storage. Access speed may be minutes, hours, or even days, depending on the access-effectiveness of the storage facility.' The principled difference between nearline data and offline data is that offline data lacks 'the coordinated control of an intelligent disk subsystem,' and is, in the lingo, JBOD ('Just a Bunch Of Disks')." (quoting CNT, *The Future of Tape 2, available at http://www.cnt.com/literature/documents/pl556.pdf.*)).

145. *Id.* ("*Backup tapes*: 'A device, like a tape recorder, that reads data from and writes it onto a tape. Tape drives have data capacities of anywhere from a few hundred kilobytes to several gigabytes. Their transfer speeds also vary considerably . . . The disadvantage of tape drives is that they are sequential-access devices, which means that to read any particular block of data, you need to read all the preceding blocks.' As a result, 'the data on a backup tape are not organized for retrieval of individual documents or files [because] . . . the organization of the data mirrors the computer's structure, not the human records management structure.' Backup tapes also typically employ some sort of data compression, permitting more data to be stored on each tape, but also making restoration more time-consuming and expensive, especially given the lack of uniform standard governing data compression." (quoting *Webopedia, at http://inews.webopedia.com/TERM/t/tape_drive.html*); (quoting Kenneth J. *Withers, Computer-Based Discovery in Federal Civil Litigation* (unpublished manuscript) at 15.) (citation omitted).

146. *Id.* ("*Erased, fragmented or damaged data*: 'When a file is first created and saved, it is laid down on the [storage media] in contiguous clusters . . . As files are erased, their clusters are made available again as free space. Eventually, some newly created files become larger than the remaining contiguous free space. These files are then broken up and randomly placed throughout the disk.' Such broken-

and 3, referred to as accessible data, and types 4 and 5, referred to as inaccessible data.[147] The court ultimately concluded that "whether production of documents is unduly burdensome or expensive turns primarily on whether it is kept in an accessible or inaccessible format."[148]

The Federal Judicial Center ("FJC") enumerated a similar distinction between five types of data. The five types, in "ascending order of cost and burden to recover and produce" are: (1) metadata;[149] (2) system data;[150] (3) backup data;[151] (4) files purposely deleted by a computer user;[152] and (5) residual data.[153] The FJC noted that, while all five types of data were discoverable, types 4 and 5 posed a unique challenge because they could only be recovered through expert intervention.

---

up files are said to be fragmented,' and along with damaged and erased data can only be accessed after significant processing.") (quoting *Sunbelt Software, Inc., White Paper: Disk Defragmentation for Windows NT/2000: Hidden Gold for the Enterprise 2, at http://www.sunbelt-software.com/evaluation/455/web/documents/idcwhit e-paper-english.pdf* (last visited May 5, 2003) (citations omitted).

147. *Id.* at 319-20.

148. *Id.* at 318 (emphasis omitted).

149. MANUAL FOR COMPLEX LITIGATION (FOURTH) § 11.446 (2004) ("Metadata, or 'information about information.' This includes the information embedded in a routine computer file reflecting the file creation date, when it was last accessed or edited, by whom, and sometimes previous versions or editorial changes. This information is not apparent on a screen or in a normal printout of the file, and it is often generated and maintained without the knowledge of the file user.").

150. *Id.* ("System data, or information generated and maintained by the computer itself. The computer records a variety of routine transactions and functions, including password access requests, the creation or deletion of files and directories, maintenance functions, and access to and from other computers, printers, or communication devices.").

151. *Id.* ("Backup data, generally stored off-line on tapes or disks. Backup data are created and maintained for short-term disaster recovery, not for retrieving particular files, databases, or programs. These tapes or disks must be restored to the system from which they were recorded, or to a similar hardware and software environment, before any data can be accessed.").

152. *Id.* ("Files purposely deleted by a computer user. Deleted files are seldom actually deleted from the computer hard drive. The operating system renames and marks them for eventual overwriting, should that particular space on the computer hard drive be needed. The files are recoverable only with expert intervention.").

153. *Id.* ("Residual data that exist in bits and pieces throughout a computer hard drive. Analogous to the data on crumpled newspapers used to pack shipping boxes, these data are also recoverable with expert intervention.").

Analogizing to the criminal context, *Zubulake* and the FJC's distinctions both suggest that the appropriate line to draw in determining which actions qualify as obstruction of justice should focus on the difficulty of accessing the relevant information. Because recovery of data located on offline backup storage, deleted, or otherwise fragmented—including "residual data" in the FJC's language—poses a unique challenge to litigants, one could likewise claim that this data has been deleted or concealed within the meaning of the obstruction of justice provisions. In other words, affirmatively moving data to an inaccessible location serves as the basis for a criminal obstruction analysis under this approach. Using spoliation as the basis for the obstruction of justice provisions closely mirrors the *Katakis* approach, which requires considering "the effort that an investigator would have to expend to uncover a hidden document."[154]

However, there is a difference of methodology between the *Zubulake*/FJC approach and that of the Ninth Circuit in *Katakis*. *Zubulake* and the FJC define accessibility in terms of how and where the data is stored. Conversely, the *Katakis* court's reasoning does not depend on how the data has been stored, but rather defines "actual obstruction" in terms of whether or not the item can be found. Although these two analyses may lead to a similar outcome in a range of cases, they differ in certain borderline cases. For example, both *Zubulake* and the FJC presume that archival data[155] is accessible, even if accessing it may prove time-consuming or otherwise challenging. The reasoning in *Katakis*, though, could lead to the conclusion that archiving data actually obstructs justice, particularly if the archived information is poorly organized, difficult to locate, or otherwise decreases the possibility that data may be found. In other words, the spoliation approach defines particular categories of data as inaccessible based on how they have been stored, whereas *Katakis* applies a more flexible approach.

This distinction highlights a lingering problem with the spoliation approach: it is heavily tied to available technology. Defining obstruction of justice in terms of a preset list of storage mediums would dramatically undercut the flexibility of courts and prosecutors to adapt to new technologies as they arise. This is perhaps most evident in *Zubulake,* as the court still discusses backup

---

154. United States v. Katakis, 800 F.3d 1017, 1030 (9th Cir. 2015).

155. *Zubulake* calls this "off-line" whereas the FJC calls this "backup data." Backup data is slightly broader, encompassing *Zubulake*'s "backup tapes," but for purposes of this section, archival data refers to data stored on a different storage device that must be connected to or restored to the primary system.

tapes as a common form of data storage, with no mention of more modern storage options such as cloud storage. Requiring courts to categorize each new data storage medium as either accessible or inaccessible could lead to a byzantine code that seems antithetical to both the reasonably flexible language of the Act and Congress's goal of punishing interference with federal proceedings and investigations.

2. Automatic Deletion

Another notable feature of ESI that frequently arises in the civil litigation context is document retention policies. Document retention policies require documents and records produced in the course of business to be stored but also specify which records should be destroyed and when in order to keep storage costs low.[156] "Organizations that destroy or discard data on an *ad hoc* basis may face serious and adverse legal consequences," as may individuals who fail to comply with a properly crafted policy.[157] Conversely, "[m]ost courts will not punish evidence destruction pursuant to an organization's policy."[158]

Although document retention policies and the obstruction of justice statutes serve conflicting purposes—the former aims to keep storage costs low while the latter seeks to preserve evidence—the two may be reconciled with a well-designed document retention program.[159] Such a program

> should be created at a *neutral* time, when litigation or an investigation is not pending or foreseeable . . . should divide each type of document or file into categories and then assign a retention period for each category . . . should also clearly describe the document destruction procedures . . . [and] should state what corporate personnel need to do when litigation or an investigation commences . . . .[160]

Even for more advanced document retention policies which automatically delete old files or e-mails, "upon receipt of a

---

156. M. James Daley & Michael L. Koon, *E-Discovery and Corporate Liability Under Sarbanes-Oxley and Criminal Obstruction of Justice Statutes*, A.L.I. - A.B.A. 361, 363 (2006).

157. *Id.* at 366.

158. Chase, *supra* note 82, at 728.

159. *Id.* at 756.

160. *Id.* at 756-57 (footnotes omitted) (emphasis added).

subpoena, the company should disable any automatic IT functions and halt any routine IT practices that risk the loss or destruction of potentially responsive ESI . . . [and] disable the "auto-delete" function on email servers and halt the common practice of "over-writing" server back-up tapes."[161]

These document retention guidelines could serve as useful guidelines for determining which activities may violate the obstruction of justice statute. For example, if, before any federal proceeding or investigation is foreseeable, a person decides to encrypt all files or automatically clear their browser history after each session as a default setting on their laptop, then such activities would not constitute obstruction of justice since the decision was made at a "neutral time." Even if, at a later point, incriminating files were encrypted or browser history was deleted, that would be an automatic occurrence, not concealment or destruction by the defendant.

There are a number of problems with this approach. Most significantly, compliance with a document retention policy usually negates the *mens rea* component of the statute, not the *actus reus* of destruction or concealment.[162] However, if one views an automatic deletion carried out because of a default setting as distinct from the active erasure of information from a computer by a user, then automatic processes would not satisfy the *actus reus* either, even if the user knows and is taking advantage of that setting, because they are not actually carried out by a person; rather, they are done by the computer.[163] Just as a person does not play a role in determining which deleted data is overwritten when a new file is saved, permitting an automatic program to run likely does not fit within the

---

161. MARK P. GOODMAN & DANIEL J. FETTERMAN, DEFENDING CORPORATIONS AND INDIVIDUALS IN GOVERNMENT INVESTIGATIONS. § 18.3 (2014-2015 ed. 2014).

162. *See* Chase, *supra* note 82, at 758-59 ("Once an appropriate policy is in place, the best argument a corporation can make in order to reconcile its policy with obstruction statutes is that because of a consistently applied and routinely followed retention policy, the corporation did not have the specific intent to obstruct justice as required by federal law.").

163. One exception to this view would be if the default were set at a time when one had the requisite *mens rea* to impose criminal liability because then the default would not be created at a neutral time. For example, if an accountant decides to encrypt all emails to his clients as a security measure and then ultimately commits fraud via email at some later time, he could not be held liable for obstruction of justice. Conversely, if he decides to start encrypting all of his emails because he is considering committing fraud, this would still qualify as obstruction.

actus reus of destruction or concealment because it is wholly passive conduct. Even if a person knows that, by not deactivating certain default settings, some information material to an investigation will be lost, the failure to stop an automatic process does not fit within the definition of the acts listed in the statutes.

G. An Alternative Approach

Given the different shortcomings of the aforementioned approaches, this Note argues that the best way to define the *actus reus* of obstruction of justice requires drawing on both the *Katakis* and spoliation approaches while refocusing the inquiry on the defendant's actions. The goal of this alternative approach is to combine the flexibility of the *Katakis* approach with the sharp lines of the spoliation approach, while avoiding the technology-specific aspects of both. This definition will involve two broad considerations, both borrowed from the spoliation approach, and this section will consider both in turn.

First, to qualify as obstruction of justice, the electronic or digital records and documents at issue must have been destroyed, concealed, or mutilated by the actions of a user, not because of any default settings. Second, the document or record must be wiped, or at least partially overwritten, for it to have been destroyed or mutilated within the meaning of the statute. Similarly, concealment requires that the file be either actually deleted or moved to a different device. The precise contours of these definitions will be discussed more thoroughly below.

3. Manual Deletion

The first requirement of this proposed definition—that the relevant file be manually, as opposed to automatically, deleted or concealed—stems from both the spoliation context and a problem flagged by the Ninth Circuit in *Katakis*. As noted above, sanctions for spoliation usually can only be imposed for failure to adhere to an established document retention and destruction policy.[164] Permitting the deletion of files after a certain period of time makes sense, not only because it keeps storage costs low, but also because deciding in each instance which file to keep and which to delete would prove incredibly time-consuming and difficult. Moreover, some files can be presumed to be useless because they have not been accessed in a significant period of time. For example, the

---

164. *See* Daley & Koon, *supra* note 156, at 366.

default setting on Gmail is to delete emails in the trash or spam folders after 30 days.[165]

Excising this category of deletions from the purview of the obstruction of justice statute would prevent prosecutions for actions that are not undertaken by a defendant in any meaningful way. Many people do not change their default settings with any frequency and, even if they are aware of them, may not be able to change them. But, even if a tech-savvy defendant changes the default settings on their browser so that at the end of every session the browser history is cleared, such activity still should not satisfy the *actus reus* requirement of the obstruction of justice provisions. With default settings, one cannot say that the defendant actively participated in the deletion of a file; rather, he permitted his computer to do so. In the same way that effective document retention policies define how and when to destroy documents at a "neutral time" prior to any foreseeable investigations or litigation,[166] picking certain settings on a computer prior to any foreseeable proceeding should insulate individuals from prosecution for information lost in accordance with that setting.[167]

One complication with this approach is that, in the spoliation context, document retention policies must be suspended once litigation arises, whereas in the above formulation, there would be no duty to change the default settings once a criminal investigation becomes foreseeable. However, given the statutory language, neither § 1512(c) nor § 1519 imposes a duty to preserve evidence; rather, they criminalize the destruction of evidence.[168] Moreover, spoliation leads primarily to civil sanctions whereas Sarbanes-Oxley carries a penalty of up to twenty years in prison; therefore, it is reasonable to be more lenient towards criminal defendants than adverse parties in a civil suit.

---

165. *See About Gmail*, GOOGLE, https://www.google.com/mail/help/tips.html, (last visited Jan. 31, 2016, 4:25 PM).

166. *See* Chase, *supra* note 82, at 756.

167. For example, a student who decides to encrypt their email while in school and, years later, uses that encrypted email account to commit fraud could not be charged with obstruction of justice. Conversely, a person who sets up an encrypted email account for the purpose of committing fraud could be prosecuted because that person knew he or she was using the encrypted account to engage in criminal activity that could foreseeably be investigated.

168. Although §§ 1512 and 1519 only criminalize destruction, 18 U.S.C. § 1520 actually does impose a statutory recordkeeping requirement. However, § 1520 explicitly applies only to accountants, suggesting that mandatory recordkeeping or file preservation is not inherent in the other obstruction of justice sections.

This approach is also slightly at odds with the language in *Katakis*. The Ninth Circuit suggested that moving incriminating emails to a trash folder did not count as obstruction because items in the trash folder were not automatically deleted.[169] But the court itself pointed out that, in the analogous situation of a real world trash can, "[i]t is nonsensical that . . . the incriminating appointment book could have been actually destroyed simply by placing it a trash can."[170] This suggests that merely placing an item where it may later be destroyed is not in and of itself obstruction unless further action is taken to ensure the item's destruction. Similarly, relying on certain settings, whether they be automatic encryption or deletion of browser history, is not the same as concealing or destroying a file.

4. Wiping, Overwriting, and Deleting as Destroying, Mutilating, and Concealing

The second requirement of this alternative approach would define the relevant statutory terms—destroy, mutilate, and conceal—in terms of specific actions—namely, wiping, overwriting, and deleting, respectively.

Looking first at the terms "destroy" and "mutilate," wiping or partially overwriting comports with both the statutory language and prior applications of the statute. As noted above, both destroy and mutilate indicate a high level of tampering. To destroy an object means to render it "unusable, unrepairable, or nonexistent."[171] Likewise, to mutilate something is to "render seriously defective by destroying or removing a material part."[172] Although at first glance these definitions may not easily transfer to the digital context, they do have relatively clear analogs in wiped and overwritten data. Deleting a file does not actually remove it from the device, but rather marks the space occupied by that file as empty.[173] However, once that space is marked as empty, it may be gradually overwritten, rendering the deleted file unusable as portions of it are replaced by other data.[174] While this process will inevitably occur throughout a

---

169. United States v. Katakis, 800 F.3d 1017, 1029 (9th Cir. 2015).

170. *Id.* at 1029, n.6 (discussing United States v. Lessner, 498 F.3d 185, 196 n.5 (3d Cir. 2007).).

171. *Destroy*, BLACK'S LAW DICTIONARY (10th ed. 2014).

172. *Mutilate*, BLACK'S LAW DICTIONARY (10th ed. 2014).

173. *See* Axelrod et al., *supra* note 91, at 20-21.

174. *Id.*; *see also Definition of: overwrite*, PCMAG, http://www.pcmag.com/encyclopedia/term/48696/overwrite (last visited Jan. 31, 2016, 6:31 PM).

device's life as files are deleted and created, programs are available that will wipe hard drives by overwriting all of the data on the drive with random information, rendering the underlying data unreadable. This overwriting process embodies the definitions of mutilation and destruction provided above because it renders the information unusable or seriously defective.

Concealing digital data, however, proves much easier. Because deleting a file removes the location of the file from the directory, such an action would likely qualify as "intentional or injurious suppression . . . of facts" as well as "removing from sight or notice,"[175] i.e. concealment. However, the file must actually be deleted, not just moved to a deleted items folder or recycling bin, as was the case in Katakis.[176] Moving a file to a different folder simply changes its address or location on the computer, but it does not necessarily make it more difficult to locate and does not remove it from sight, since the file could still be found in the directory. Concealing digital information, then, involves removing the reference or pointer to the location where the file is stored because that renders the file inaccessible by the computer, even though it is still technically present on the hard drive. Consequently, deleting a file from a computer but storing it on a CD, flash drive, or external hard drive would still count as concealment because the information would not be accessible by the computer without connecting or inserting the external storage device and therefore would be removed from the "sight or notice" of the computer.[177] At a higher level of generality, concealment means rendering information inaccessible, but leaving it intact and usable if discovered. Therefore, encrypting information would obviously qualify as concealment, as the information would be inaccessible without the key necessary to decrypt it, but would remain uncorrupted and readable if the key could be obtained.[178]

This approach leaves undisturbed many of the cases discussed above that involve the deletion of digital data. Wiping hard drives

---

175. *Concealment*, BLACK'S LAW DICTIONARY (10th ed. 2014).

176. United States v. Katakis, 800 F.3d 1017, 1029 (9th Cir. 2015).

177. In the words of the *Zubulake* court, moving data from "online" or "near-line" to "off-line" would qualify as concealment, because the data would not be automatically accessible by the computer. This moves the line slightly as compared to the civil litigation context and actually is slightly broader than the test applied by the *Zubulake* court, which concluded that data backed up to a separate device was inaccessible whereas merely off-line data was not. This approach is actually in line with the FJC's approach, which likewise considers data deleted by the user as posing a special challenge to accessibility.

178. For an overview of basic encryption techniques, *see* NETWORK ASSOCS., INC., AN INTRODUCTION TO CRYPTOGRAPHY, 11-36 (1990).

clearly falls within the compass of "destroying" records, but other obstructive acts, such as encrypting or deleting a file, would qualify as concealment. This definition, however, excludes certain acts: deleting an email or file but leaving it in a trash folder or recycling bin would not qualify as obstruction of justice. Likewise, if a file is stored in the cloud,[179] then deleting a local version of the file may not qualify as concealment if the file could just as easily be accessed in the cloud, assuming the computer is connected to the Internet. Conversely, actually removing a file from the server and rendering it inaccessible would qualify as obstruction, even if another computer within the network might still have a local version of the file.

Cloud computing, along with other wholly web-based accounts and information storage services, provide a helpful illustration of how the principles expounded above might apply. "In the simplest terms, cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive."[180] In that sense, the cloud is similar to removable storage media, such as flash drives or external hard drives, as it provides a separate location that stores data but that may still be accessed from a connected device. Just as plugging a flash drive into a computer enables a user to view the files on the drive, connecting to the Internet enables a user to access files stored in the cloud. Therefore, if a device is set up such that it automatically accesses files stored on the cloud whenever it connects to the Internet—i.e. the cloud storage is not password protected and the user does not have to switch on the connection between the local device and the cloud server—then deleting a locally saved copy of the file would not amount to obstruction, because the cloud-based version would be easily accessible.[181] Conversely, if, for example, a user's Dropbox account were password protected such that a password had to be entered every time someone tried to access a document stored on the cloud, then deleting a local copy may qualify as obstruction, as the file

---

179. For a useful summary of what the cloud is, how it works, and some of the issues raised by cloud computer, *see* Eric Griffith, *What is Cloud Computing?*, PCMAG (May 3, 2016), http://www.pcmag.com/article2/0,2817,2372163,00.asp.

180. *Id.*

181. This analysis mirrors the discussion of automatic deletion above. Just as automatic deletion or encryption should not provide grounds for an obstruction charge, automatic connection to the cloud means that deletion of a local file cannot serve as the predicate act for an obstruction charge.

could not be accessed by the computer without additional user input and, in that sense, is not accessible by the computer.[182]

The approach discussed in this section also faces a number of other issues, in addition to the ones generated specifically by the cloud. To some extent, it generates surplusage in the statutory language, since it essentially collapses the distinction between destroy and mutilate. However, since the law does not solely apply in the digital realm but also applies to physical objects where a clearer distinction exists between mutilation and destruction, this is not a pressing concern. More significantly, while the definition strives to be technology-neutral and use terminology that applies across devices, it is inevitably moored to present technological conceptions. Technology will change in the near future, and it may render processes like overwriting obsolete or unnecessary. Unfortunately, writing a definition that encompasses all possible technological change remains nearly impossible.

Nevertheless, this approach has the substantial benefit of returning the focus of any future case to the conduct of the defendant. Regardless of how likely a deleted document is to be found or how recoverable an erased file is, if the defendant engages in particular conduct, then they have obstructed justice. The skills of the investigators and the particular storage medium involved are no longer relevant to the inquiry.

V. CONCLUSION

Even though §§ 1512(c) and 1519 were written well after computers and the Internet permeated countless aspects of daily life, the provisions still failed to properly account for the range of obstructive conduct that may occur in the digital world. Prosecutors have opted to wield the nebulous language of these new obstruction of justice provisions to criminalize a wide variety of conduct. While these statutes have not yet swept up a significant amount of largely innocent conduct, they have the potential to make even the most

---

182. This approach draws a very fine line that may strike some as overly formalistic—automatically connecting to the cloud protects one from charges, but entering a password subjects an individual to a twenty-year sentence. Similarly, this reasoning suggests that a laptop found with a flash drive plugged in would not raise obstruction of justice issues, but a laptop with an unplugged flash drive sitting next to it might. Nevertheless, this distinction presents one of the only principled and consistent lines that may be drawn and accords with the case law and statutory language, even if it raises some troubling implications. Ultimately, this issue is probably best handled by looking to whether the defendant had the requisite intent to obstruct.

mundane of activities illegal. Therefore, imposing some limits on the expansive language is necessary. Specifically, requiring that acts occur manually, instead of as the result of a default setting, and that the information actually be rendered inaccessible or unreadable and unusable, would help mitigate some of the negative outcomes of an overly-broad law while allowing law enforcement to prosecute those who actually obstruct justice.