Trespass, Not Fraud: The Need for New Sentencing Guidelines in CFAA Cases

*Orin S. Kerr**

Abstract

This Article argues that the existing regime for sentencing violations of the Computer Fraud and Abuse Act ("CFAA") is based on a conceptual error that consistently leads to improper sentencing recommendations. The Federal Sentencing Guidelines treat CFAA violations as economic crimes. Most CFAA crimes are rooted in trespass, however, instead of economic wrongs such as fraud. The difference is significant. The economic crimes framework leads guidelines calculations to focus too much on economic loss and not enough on the circumstances of the crime. The Article concludes by sketching out a better way to calculate sentencing recommendations in CFAA cases.

Table of Contents

* Fred C. Stevenson Research Professor, The George Washington University Law School. Thanks to Doug Berman, Shon Hopwood, Michael Levy, and the participants at *The George Washington Law Review* Symposium for comments on an earlier draft.

INTRODUCTION

The Computer Fraud and Abuse Act ("CFAA")[1] is controversial in part because its punishments are widely perceived as draconian. Some of those perceptions are the result of flawed reporting. Media coverage of CFAA prosecutions routinely emphasizes statutory maximum sentences instead of Federal Sentencing Guidelines recommendations, fostering wildly unrealistic perceptions of likely punishments.[2] But part of the perception is accurate, and it results from the quirky way the Guidelines characterize CFAA offenses. Sentencing recommendations for CFAA crimes are calculated using the economic crimes guideline, section 2B1.1.[3] That guideline hinges sentencing recommendations primarily on the victim's consequential loss.[4] A focus on loss makes sense for sentencing economic crimes such as theft. That approach is inappropriate in most CFAA prosecutions, however, because they involve a different set of harms.

This Article argues that the Sentencing Commission should rewrite the Guidelines for CFAA cases because the current approach is based on a conceptual error. Most CFAA offenses are trespass offenses, not economic crimes.[5] The primary harm in most CFAA cases

---

1 Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (2012).

2 *See, e.g.*, Justin Wm. Moyer, *'Beyond Disgusting,' Says Journalist Matthew Keys of His Hacking Conspiracy Conviction*, WASH. POST (Oct. 8, 2015), https://www.washingtonpost.com/news/morning-mix/wp/2015/10/08/edward-snowden-miffed-journalist-facing-years-in-prison-for-conspiring-to-deface-an-online-newspaper-article/ [https://perma.cc/ADR5-U2WA] (stating that "the end result [of a CFAA conviction] may mean 25 years in prison," the statutory maximum in that case); *Harvard Uni Fellow Faces 35 Years Jail for 'Stealing 5m Academic Online Articles Dating From 17th Century*,' DAILY MAIL (July 20, 2011, 8:16 AM), http://www.dailymail.co.uk/news/article-2016852/Harvard-Uni-fellow-faces-35-YEARS-jail-stealing-5m-academic-online-articles-dating-17th-century.html ("A Harvard University ethics fellow faces 35 years in jail after over [sic] accusations he hacked into the Massachusetts Institute of Technology computer network to steal nearly 5million [sic] academic articles.").

3 U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 (U.S. SENTENCING COMM'N 2015). Under *United States v. Booker*, 543 U.S. 220 (2005), the Guidelines are advisory rather than mandatory, but nonetheless exert a significant influence on sentencing outcomes. *See id.* at 245–46.

4 *See, e.g.*, United States v. Millot, 433 F.3d 1057, 1061 (8th Cir. 2006).

5 *See generally* Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143

is invasion of privacy and interference with the right to exclude, not economic loss. Although CFAA offenses can cause economic losses, their extent is usually a matter of bad luck rather than design.[6] The result is a poor fit between many CFAA crimes and the current Guidelines. Assumptions about how to measure culpability built into section 2B1.1 often misfire when applied to CFAA crimes. Applying the Guidelines can lead to sentences far removed from what the goals of punishment would suggest are appropriate.[7]

The Sentencing Commission should take a fresh approach. First, it should enact a new guideline for convictions under the computer trespass sections of the CFAA, 18 U.S.C. § 1030(a)(2)–(3) and (a)(5)(B)–(C). The new guideline should account for consequential losses, but only as a small adjustment rather than the sledgehammer it plays in the current economic crimes guideline. Second, the Sentencing Commission should continue to use the economic crimes guideline for convictions under the fraud and intentional damage sections of the CFAA, § 1030(a)(4)–(5)(A), but it should amend that guideline to better treat CFAA offenses. Finally, the Sentencing Commission should narrow the use of the sophisticated means and special skills enhancements in CFAA cases.

Part I of this Article explains the evolution of the CFAA-related sentencing guidelines. Part II argues that the current approach is a poor fit for many CFAA offenses. Part III sketches out new principles that should guide sentencing for CFAA crimes.

I. A Brief History of CFAA Sentencing

The CFAA codifies several different, but often overlapping computer-misuse offenses. The three most important crimes are unauthorized access to obtain information banned by 18 U.S.C. § 1030(a)(2); unauthorized access to commit a fraud prohibited by 18 U.S.C. § 1030(a)(4); and computer damage criminalized by 18 U.S.C. § 1030(a)(5). When a defendant is convicted of one or more of these

(2016) (discussing the use of trespass norms as "a framework to distinguish between authorized and unauthorized access to a computer").

6 *See* Jennifer S. Granick, *Faking It: Calculating Loss in Computer Crime Sentencing*, 2 I/S: J.L. & Pol'y Info. Soc'y 207, 214–18 (2006).

7 *See* 18 U.S.C. § 3553(a)(2) (2012) (listing the goals to be served by criminal punishment that should govern sentencing); *see also* Hanni Fakhoury, *How the Sentencing Guidelines Work Against Defendants in CFAA Cases*, Electronic Frontier Found. (Apr. 9, 2013), www.eff.org/deeplinks/2013/03/41-months-weev-understanding-how-sentencing-guidelines-work-cfaa-cases-0 [https://perma.cc/R8GC-P63R].

offenses, the sentencing court will apply the economic crime guideline, section 2B1.1, to calculate a recommended sentence.[8]

This Section explains how the Sentencing Commission came to adopt the current approach to sentencing CFAA crimes. The Sentencing Commission initially treated CFAA offenses like fraud crimes. Over time, it adopted a broader approach that I will call "fraud plus." Under the "fraud plus" approach, punishments are based heavily on a loss chart combined with additional CFAA-specific adjustments.

A. The Initial Fraud Approach

The Guidelines went into effect in 1987.[9] At the time, the CFAA was new. 18 U.S.C. § 1030 had been introduced as a very narrow statute in 1984, and it was expanded considerably in 1986.[10] The first statutory index published with the initial Guidelines did not have an entry for the CFAA.[11] Starting in January 1988, however, the statutory index directed that convictions under the three major sections of the CFAA, § 1030(a)(2) and (4)–(5), should be sentenced under the then-existing fraud provision, section 2F1.1.[12] This meant that CFAA sentences would be calculated like any fraud crime.

Although we can only speculate about why the Sentencing Commission chose to sentence CFAA crimes under the fraud guideline, it probably seemed like a natural choice. In the first twelve years of the statute, from 1984 through 1996, there were only 174 CFAA convictions—an average of about fifteen cases a year.[13] The small number of cases presumably encouraged use of a preexisting guideline. And if a preexisting guideline was to be employed, the fraud guideline must have seemed a sensible if not obvious selection. The 1984 law that created 18 U.S.C. § 1030 had been titled the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984.[14] It had directed

---

8 *See* U.S. SENTENCING GUIDELINES MANUAL app. A.

9 *See* United States v. Polk, 905 F.2d 54, 55 (4th Cir. 1990) (citing Sentencing Reform Act of 1984, ch. II, sec. 235(a)(2), § 4, 99 Stat. 1728.).

10 *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1563–67 (2010).

11 *See* U.S. SENTENCING GUIDELINES MANUAL app. A (U.S. SENTENCING COMM'N 1987) (in a list of ordered federal crimes associated with specific guidelines, skipping from 18 U.S.C. § 1029 to 18 U.S.C. § 1071).

12 *See* U.S. SENTENCING GUIDELINES MANUAL app. A (U.S. SENTENCING COMM'N 1988).

13 *See* U.S. SENTENCING COMM'N, ADEQUACY OF FEDERAL SENTENCING GUIDELINE PENALTIES FOR COMPUTER FRAUD AND VANDALISM OFFENSES 2 n.3 (1996).

14 Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98. Stat. 2190.

the new statute to be inserted into chapter 47 of title 18,[15] which is the "fraud and false statements" section of the criminal code.[16] The 1984 law had also given 18 U.S.C. § 1030 its caption: "Fraud and related activity in connection with computers."[17] Based on the statute's name, caption, and its location in title 18, it probably seemed natural to treat 18 U.S.C. § 1030 as a fraud statute sentenced under the fraud guidelines.

This choice made CFAA sentences almost entirely dependent on the "loss" triggered by the offense. The Guidelines recommend a sentence based on the offense level, which is reached by beginning with a base offense level appropriate for that crime and then adjusting the offense level based on the circumstances.[18] The then-existing guideline for fraud cases, section 2F1.1, consisted mostly of a loss chart that set the sentence based on how much loss was caused.[19] The more loss the crime caused, the greater the punishment.[20] Using the 1992 version of the Guidelines as an example, a loss of between $40,000 and $70,000 would add five levels; a loss of $10 million to $20 million would instead add fifteen levels.[21] At the time, the Guidelines commentary explained that the meaning of "loss" was taken from the theft and larceny guideline, section 2B1.1, and that it was an attempt to measure "the value of the money, property, or services unlawfully taken."[22] The framework makes intuitive sense for a theft crime. The more you steal, the more punishment you deserve.

B. Department of Justice Proposes "Fraud Plus"

In 1993, the Department of Justice ("DOJ") criticized this approach as insufficiently punitive.[23] According to the DOJ, the fraud guidelines did not clearly capture all the harms caused by computer intrusions.[24] First, they did not include nonmonetary harms such as privacy invasions.[25] Second, computer intrusions caused consequential harms not clearly encompassed by section 2F1.1, such as the costs

15 *Id.*

16 18 U.S.C. §§ 1001–40 (2012).

17 Counterfeit Access Device and Computer Fraud and Abuse Act § 2102.

18 U.S. SENTENCING GUIDELINES MANUAL ch. 1, pt. A (U.S. SENTENCING COMM'N 2015).

19 *See* U.S. SENTENCING GUIDELINES MANUAL § 2F1.1 (U.S. SENTENCING COMM'N 1990).

20 *Id.*

21 *See* U.S. SENTENCING GUIDELINES MANUAL § 2F1.1 (U.S. SENTENCING COMM'N 1992).

22 *Id.* § 2F1.1 cmt. n.7.

23 *See* WIN SWENSON ET AL., COMPUTER FRAUD WORKING GROUP REPORT 3 (1993).

24 *See id.*

25 *See id.*

of restoring the network following a breach.[26] In response, the DOJ proposed a new guideline for § 1030 offenses to be codified at a proposed section 2F2.1, which would include these additional harms.[27]

I will call the DOJ's recommended approach "fraud plus," as it treats CFAA offenses as fraud crimes for loss purposes and then adds additional punishment for other attributes of the offense. The DOJ recommended two specific steps to enact this approach. The first proposal was to retain the section 2F1.1 loss chart but add a special directive for how to calculate losses in CFAA cases.[28] According to the proposal, CFAA losses should include "costs accrued by the victim in identifying and tracking the defendant, ascertaining the damage, and restoring the system or data to its original condition . . . . [A]s well as losses incurred from interruptions of service."[29]

Second, the DOJ proposed adjustments for specific kinds of facts in CFAA cases.[30] The proposal recommended a two level adjustment for obtaining information; a four level increase for distributing information; a six level adjustment for distributing information "by means of a general distribution system;"[31] and a six level adjustments for "interference with the administration of justice (civil or criminal) or harm to any person's health or safety"[32] and "interference with any facility (public or private) or communications network that serves the public health or safety . . . ."[33] The basic idea was to add adjustments beyond the loss chart for CFAA offenses that involved particular harms.

In response to DOJ's proposal, the Sentencing Commission formed a Computer Fraud Working Group that published an extensive report in 1993.[34] The Working Group agreed with DOJ's views about the need for revised amendments, but it concluded that the Sentencing Commission should introduce the amendments directly into the existing section 2F1.1 rather than create a separate guideline just for CFAA offenses.[35]

---

26 *See id.*

27 *See id.*

28 *See* Sentencing Guidelines for United States Courts, 57 Fed. Reg. 62,832, 62,855–56 (proposed Dec. 31, 1992).

29 *Id.* at 62,856. The Sentencing Commission published DOJ's proposal as a proposed amendment. *See id.* at 62,855–56.

30 *See id.* at 62,855–56.

31 *Id.* at 62,855.

32 *Id.*

33 *Id.*

34 *See* SWENSON ET AL., *supra* note 23.

35 *See id.* at 26–28.

C. *The Sentencing Commission Eventually Adopts "Fraud Plus"*

Over time, the guidelines applicable to CFAA crimes were amended to adopt the basic approach of the DOJ's 1992 proposal. Consistent with the Working Group's recommendation, the changes were added to the existing Guidelines instead of presented as a separate guideline just for CFAA offenses. But consistent with the DOJ's proposal, the Sentencing Commission adopted the "fraud plus" approach that included broad consequential losses as well as additional adjustments.

The changes happened piecemeal. First, in 1997, the Guidelines added specific guidance that included at least some consequential losses as losses in CFAA cases.[36] According to the guidance, loss in CFAA cases was to include "the reasonable cost to the victim of conducting a damage assessment, restoring the system and data to their condition prior to the offense, and any lost revenue due to interruption of service."[37]

This language was expanded in 2001, when the Sentencing Commission merged the fraud guideline of section 2F1.1 and the theft guideline of section 2B1.1 into the unified economic crimes guideline found in section 2B1.1.[38] The 2001 economic crimes guideline clarified that loss is the greater of actual or intended loss, with actual loss defined as "reasonably foreseeable pecuniary harm."[39] But in the case of CFAA offenses, the guideline introduced a special rule: consequential losses were included even if they were not reasonably foreseeable.[40]

The guidelines for CFAA offenses were expanded again in 2003 in response to a 2002 congressional directive for the Sentencing Commission to "review and, if appropriate, amend its guidelines" for § 1030 offenses to "reflect the serious nature" of such crimes including "the potential and actual loss resulting from the offense."[41] The 2003

---

36 *See* U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 cmt. n.2 (U.S. SENTENCING COMM'N 1997). In 1997, the statutory index was also changed so that not all of the core § 1030(a) offenses were linked to the fraud guideline. *See id.* app. A. At the time, § 1030(a)(2) was linked to section 2B1.1, § 1030(a)(4) was linked to section 2F1.1, and § 1030(a)(5) was linked to section 2B1.3. *See id.*

37 *See id.* § 2B1.1 cmt. n.2.

38 *See* Frank O. Bowman, III, *The 2001 Federal Economic Crime Sentencing Reforms: An Analysis and Legislative History*, 35 IND. L. REV. 5, 7 (2001).

39 U.S. SENTENCING GUIDELINES MANUAL §2B1.1 cmt. n.2(A)(i) (U.S. SENTENCING COMM'N 2001).

40 *Id.*

41 Homeland Security Act of 2002, Pub. L. 107-296 § 225(b), (c), 116 Stat. 2135, 2156 (codified at 6 U.S.C. § 145 (2012)).

amendments brought the CFAA-specific provisions of section 2B1.1 close to their current form. Under the current version of section 2B1.1, the consequential losses for CFAA offenses match the 2001 statutory definition of loss adopted in the CFAA.[42] The guideline now reads:

> In the case of an offense under 18 U.S.C. § 1030, actual loss includes the following pecuniary harm, regardless of whether such pecuniary harm was reasonably foreseeable: any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service.[43]

Under the section 2B1.1 loss chart, losses can add levels to the Guidelines calculation: as little as two extra levels for a loss more than $6500 up to $15,000 to as high as thirty extra levels for a loss more than $550 million.[44]

Section 2B1.1 now also includes special adjustments for specific kinds of CFAA offenses. First, if a CFAA offense "involved an intent to obtain personal information" or "the unauthorized public dissemination of personal information," the calculation is increased by two levels.[45] Second, the calculation should be increased by the greatest of the following three applicable enhancements: if the offense "involved a computer system used to maintain or operate a critical infrastructure, or used by or for a government entity in furtherance of the administration of justice, national defense, or national security," enhance two levels; if the defendant was convicted under 18 U.S.C. § 1030(a)(5)(A), enhance four levels; and if the offense "caused a substantial disruption of a critical infrastructure," enhance six levels and increase the offense level to twenty-four if it has not already reached that level.[46]

Section 2B1.1 also recommends considering upward departures when the calculated offense level "substantially understates the seri-

---

42 18 U.S.C. § 1030(e)(11) (2012).

43 U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 cmt. n.3(A)(v)(III) (U.S. SENTENCING COMM'N 2015).

44 AMENDMENTS TO THE SENTENCING GUIDELINES § 2B1.1 (U.S. SENTENCING COMM'N 2015). These figures are from the amended loss chart that went into effect on November 1, 2015. *See id.*

45 U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(17).

46 *Id.* § 2B1.1(b)(18).

ousness of the offense."[47] Several of the examples listed in the Application Note specifically mention the CFAA. For example, an upward departure may be appropriate in a CFAA case if the defendant stole information and "sought the stolen information to further a broader criminal purpose."[48] In a CFAA case involving damage, "an upward departure would be warranted . . . if the offense resulted in serious bodily injury or death . . . ."[49]

Today, all of the core CFAA offenses—all convictions under § 1030(a)(2) and (4)–(5)—are sentenced using section 2B1.1.[50] Courts calculate losses, including consequential losses, and apply the loss chart, and they then apply the added CFAA-specific adjustments based on the circumstances of the offense.

II. Hacking Is Not Fraud: The Poor Fit Between CFAA Crimes and the Current Guidelines

With the history of the CFAA guideline explored, we can now see how the treatment of CFAA offenses under the existing guideline is based on a conceptual mistake. Although some CFAA offenses resemble fraud crimes, many others are about trespass. The result is an awkward fit between many CFAA offenses and the guidelines recommendations. The seriousness of CFAA trespass crimes is not accurately measured by the economic crimes guideline, and CFAA fraud crimes should be punished just as frauds, rather than with the special rules for consequential losses and adjustments for CFAA offenses. The "fraud plus" approach of the existing guideline often leads to quirky results that are hard to justify using traditional principles of punishment.

This Part explains the problem with the current Guidelines in five steps. First, it explains why the loss chart approach used by section 2B1.1 is generally appropriate for economic crimes such as theft and fraud. Second, it argues that most CFAA offenses are trespass crimes, not economic crimes. Third, it shows how the existing Guidelines are a poor fit for CFAA trespass crimes. Fourth, it shows how section 2B1.1 can lead to sentences that are hard to square with the goals of punishment. Finally, it argues that courts have improperly relied on the sophisticated means and special skills enhancements in routine CFAA cases.

---

47 *Id.* § 2B1.1 cmt. n.20(A).

48 *Id.* § 2B1.1 cmt. n.20(A)(v).

49 *Id.* § 2B1.1 cmt. n.20(A)(ii).

50 *Id.* app. A.

A. Sentencing Based Heavily on Loss Amounts Is Generally Appropriate in Theft and Fraud Cases

The purpose of the economic crimes guideline is to identify appropriate punishments when economic loss is the primary harm of a federal offense.[51] The punishments calculated by the Guidelines should adequately deter future offenses, but not overdeter them; they should punish morally culpable conduct adequately, but not too harshly.[52] When economic loss is the primary harm caused by a crime, recommending sentences based heavily on an escalating loss chart usually serves those goals.[53] The loss generally will be based on the value of the property taken, and the value of the property taken generally will reflect the severity of the crime and the culpability of the criminal.[54]

Consider a simple fraud prosecution. If I defraud you of $10,000, you lose $10,000 and I gain $10,000. The primary harm is an economic loss that usually is equivalent to the defendant's unjust gain.[55] In such cases, relying on loss charts as a major determinant of the sentence recommendation usually satisfies both deterrent and retributive goals of punishment. From a deterrence perspective, reliance on a loss chart provides an incentive to minimize loss. People usually know what they are taking and roughly how valuable it is. That knowledge allows them to have some control of the loss amount. Relying on an escalating loss chart discourages the seeking of additional unjust gains.

From a retributive standpoint, reliance on a loss chart to estimate sentences for economic crimes often makes sense because losses can correlate with the moral culpability of the offense.[56] Stealing property from someone denies that person the use of that property. The more valuable the items taken, the more denial typically occurs. The greater the denial, the more culpable the act.[57] If I steal $1, I have committed only a de minimis offense. If I steal $1000, the crime is much more serious. And if I steal $10 million, the crime is vastly more serious again.

This does not mean that the existing economic crimes guideline is perfect for traditional fraud crimes. As recent debates over section

---

51 *See* Bowman, *supra* note 38, at 38.

52 *See generally* 18 U.S.C. § 3553 (2012) (providing the factors and other considerations for imposing a sentence).

53 *See* Bowman, *supra* note 38, at 39.

54 *See id.* at 39.

55 *See id.* at 47–48, 54.

56 *See id.* at 38–41.

57 *See id.* at 38.

2B1.1 suggest, any particular loss chart will imply judgments about the precise link between loss amounts and the seriousness of an offense that can be questioned in some cases.[58] Instead, my point is conceptual: the idea of basing the sentence heavily on loss generally makes sense for economic crimes.

B. Most CFAA Offenses Are Trespass Crimes, Not Economic Crimes

CFAA offenses generally present a different dynamic. Consider the heart of the CFAA, the four offenses found in 18 U.S.C. § 1030(a)(2)–(5). The core principle shared by most of those offenses is unauthorized access to a protected computer.[59] The CFAA prohibits unauthorized access to obtain information,[60] unauthorized access to a government computer,[61] unauthorized access that furthers a fraud,[62] and unauthorized access that causes damage.[63] The common idea, unauthorized access, is not economic loss. Instead, unauthorized access is a kind of computer trespass.[64] The core harm is the loss of exclusive control over a computer and its data.

More specifically, unauthorized access generally involves two kinds of harms. First, an unauthorized access can impair the confidentiality of data.[65] Information that was supposed to be private can be

---

58 *See, e.g.*, James E. Felman, *Reflections on the United States Sentencing Commission's 2015 Amendments to the Economic Crimes Guideline*, 27 FED. SENT'G REP. 288, 290 (2015); James E. Felman, *The Need to Reform the Federal Sentencing Guidelines for High-Loss Economic Crimes*, 23 FED. SENT'G REP. 138, 138–39 (2010); Derick R. Vollrath, Note, *Losing the Loss Calculation: Toward a More Just Sentencing Regime in White-Collar Criminal Cases*, 59 DUKE L.J. 1001, 1003 (2010); Patti B. Saris, Chair, U.S. Sentencing Comm'n, Keynote Address at the Regulatory Offenses and Criminal Law Conference: The 2015 Economic Crime Amendments 4–5 (Apr. 14, 2015), http://www.ussc.gov/sites/default/files/pdf/news/speeches-and-articles/speech_saris_20150414.pdf; David Debold & Matthew Benjamin, Essay, *"Losing Ground"—in Search of a Remedy for the Overemphasis on Loss and Other Culpability Factors in the Sentencing Guidelines for Fraud and Theft*, 160 U. PA. L. REV. PENNUMBRA 141, 141–42 (2011), https://www.pennlawreview.com/online/160-U-Pa-L-Rev-PENNumbra-141.pdf.

59 *See* 18 U.S.C. § 1030(a)(2)–(5) (2012).

60 *Id.* § 1030(a)(2).

61 *Id.* § 1030(a)(3).

62 *Id.* § 1030(a)(4).

63 *Id.* § 1030(a)(5)(B)–(C).

64 *See* United States v. Valle, 807 F.3d 508, 525 (2d Cir. 2015) ("[T]he legislative history [of the CFAA] consistently characterizes the evil to be remedied—computer crime—as 'trespass' into computer systems or data"); *see also* Kerr, *supra* note 5. I am including both "access without authorization" and conduct that "exceeds authorization" as examples of unauthorized access.

65 The three foundational goals of computer security are protecting the confidentiality, integrity, and availability of data or information. *See, e.g.*, MATT BISHOP, INTRODUCTION TO COMPUTER SECURITY 1 (2005).

exposed, resulting in serious privacy harms. This happens even if the victim does not know the offense occurred. Most computer intrusions remain secret—the wrongdoer breaks in, looks around, and collects information. The crime usually goes undetected, but the privacy invasion has nonetheless occurred. Second, unauthorized access can impair the integrity of data.[66] The integrity of data refers to whether it is what it purports to be.[67] In the rare case that the victim learns that a hacker was there, the victim will not know what the hacker did or whether important data has been altered or deleted. The potential or actual alternation of data can frustrate the owner's ability to rely on it.[68]

Neither of these harms is intrinsically economic. Although a privacy invasion can cause serious harm, that harm is not readily translated into dollars.[69] Impairing the integrity of information limits the victim's ability to rely on information that was accessed, but it likewise does not equate readily with a money loss. To the extent unauthorized access crimes cause economic loss, those losses are a consequence of the unauthorized access rather than its core.

Specifically, unauthorized access crimes can cause what I will refer to as "victim-reaction loss." In any criminal case that has reached the sentencing stage, the intrusion will necessarily be one of the rare instances in which the intrusion was identified and its scope investigated. The victim will have devoted time and resources to assessing the scope of the intrusion, returning the data to its prior state, and resecuring the network.[70] This time has economic value, and the value of that time reflects economic harm in the form of a victim-response consequential loss. Courts often calculate that loss by simply adding

---

66 *Id.*

67 As a computer science treatise explains:

> Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity includes data integrity (the content of the information) and origin integrity (the source of the data, often called authentication). The source of the information may bear on its accuracy and credibility and on the trust that people place in the information.

Id. at 3.

68 *See id.*

69 *See* Bruce E. Boyden, *Can a Computer Intercept Your Email?*, 34 CARDOZO L. REV. 669, 713 (2012) (discussing the difficulty of identifying the dollar costs of privacy invasions).

70 The statutory loss definition, which the Guidelines instruct judges to consider as loss at sentencing, describe the victim-response acts that take time and resources: "responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense." 18 U.S.C. § 1030(a)(11) (2012).

up the hours spent responding to the intrusion and multiplying those hours by an hourly rate.[71]

C. *The Mismatch Between Victim-Response Losses and the Economic Crimes Guideline*

Now we get to the heart of the problem. The economic losses made so important by section 2B1.1 are chiefly victim-response losses,[72] but those responses are not the core of CFAA trespass harms. This can lead courts to misjudge the seriousness of CFAA crimes. Treating victim-response loss as an economic harm under a theft framework amounts to a form of strict liability that punishes the defendant largely based on his good or bad luck about the victim's response to the offense. For a hacker who faces criminal prosecution for unauthorized access, sentencing recommendations under section 2B1.1 must seem surprisingly random: victim loss has no connection to defendant gain. Victim-response losses are unpredictable and usually outside the defendant's control.

The problem is that victim-response losses usually reflect a victim's priorities and comfort levels rather than an objective measurement of the seriousness of the offense.[73] When hacking goes undetected, which is usually the case, the victim-response loss is zero. If a CFAA case has been prosecuted, however, the intrusion must have been identified. How much effort a victim will devote to responding to the intrusion will vary considerably. Some victims will check everything to see the scope of the harm; others will not. Some victims take every step to make sure no other means to access the network exist; others will not. Victim response is not like repairing a car fender, where there is a relatively standard set of steps a body shop might take to make the repair. Instead, the losses will tend to reflect individual reactions of victims who will have decided in their discretion to spend more or less time and money in response to an intrusion.

Jennifer Granick has pointed to a fascinating case study of the arbitrariness of CFAA losses.[74] In 2001, the Honeynet Project announced a forensic challenge in which they invited analysts to review a compromised computer system and analyze what happened.[75] Ana-

---

71 *See, e.g.*, United States v. Millot, 433 F.3d 1057, 1061 (8th Cir. 2006).

72 *See supra* Section II.B.

73 *See* Granick, *supra* note 6, at 208.

74 *See id.* at 214–15.

75 *See id.* at 214.

lysts were told to keep tabs on how many hours it took them to review the victimized machine.[76] Among the thirteen entries submitted, the time spent to complete the analysis ranged from ten hours to more than 100 hours, with the latter hours being artificially limited by time running out on the competition.[77] Even in an artificial forensic challenge in which every participant was given identical instructions and competed to do the best analysis, the net victim loss ranged by at least a factor of ten.[78]

United States v. Auernheimer[79] provides a more recent example of the arbitrariness of victim-response losses.[80] Auernheimer had helped collect over 100,000 customer email addresses from an AT&T server.[81] After collecting the addresses, Auernheimer and his co-conspirator proudly took credit for their conduct by reporting it to the press.[82] Facing negative press attention, AT&T responded in two ways. First, AT&T emailed its customers to explain that their accounts had not been accessed and that their data was safe.[83] Second, AT&T supplemented its email notice with a postal letter repeating the email message.[84] The cost of sending the postal letter to more than 100,000 customers was estimated to be $73,000.[85]

At sentencing, the district court held that the sole loss caused by the offense was the $73,000 cost of printing and mailing the letters.[86] According to the judge, this victim-response loss fell within section 2B1.1, leading to an eight level adjustment for causing economic loss more than $70,000.[87] From the base level of six, the eight-level adjustment brought the offense level to fourteen.[88] The court then added

---

76 *Id.*

77 *Id.* at 215.

78 *See id.*

79 United States v. Auernheimer, No. 11-cr-470 (SDW), 2012 WL 5389142 (D.N.J. Oct. 26, 2012).

80 *See generally id.* The defendant's conviction was later overturned on venue grounds. *See* United States v. Auernheimer, 748 F.3d 525, 526 (3d Cir. 2014). Full disclosure: I represented the defendant on appeal before the Third Circuit. Of course, all of the viewpoints expressed in this Article represent my personal opinion.

81 *Auernheimer*, 748 F.3d at 531.

82 *See id.*

83 *See* Appellant's Opening Brief at 56, United States v. Auernheimer, 748 F.3d 525 (3d Cir. 2014) (No. 13-1816).

84 *Id.* at 2.

85 *See id.*

86 Transcript of Proceedings: Sentence at 14–15, United States v. Auernheimer, No. 11-cr-470 (SDW), 2012 WL 5389142 (D.N.J. Mar. 18, 2013).

87 *Id.*

88 *Id.*

three two-level adjustments for using special skills, using sophisticated means, and obtaining personal information to reach an offense level of twenty.[89] The Guidelines' range was thirty-three to forty-one months, and the court then sentenced Auernheimer to the top end of the Guidelines.[90]

Note what happened: the Guidelines recommended two extra years in jail because AT&T opted to mail out a postal letter. If AT&T had relied on its email notice, the loss would have been zero. The offense level would have been twelve instead of twenty. A sentence at the high end of the Guidelines would have been twenty-five months fewer—sixteen months—instead of forty-one months.[91] But Auernheimer had no way to control whether AT&T would pick the free way to notify its customers or the expensive way.

D. Section 2B1.1 and the Rationales for Punishment in Trespass Cases

The unpredictable nature of victim-response losses in unauthorized access cases makes heavy reliance on those losses at sentencing inappropriate. Under section 2B1.1, the defendant is not judged by his act but by the victim's response. Numbers such as how many hours the victim spent and the hourly rate of the employees who did the work determine the jail sentence that the defendant is likely to receive.[92]

From a deterrent perspective, however, basing the punishment on reactions generally outside of a defendant's control is troublesome. In theft cases, a defendant has significant control over economic loss. The threat of higher punishment for greater loss can encourage steps that minimize loss. But because computer trespass defendants have little way to control victim-response losses, no such encouragement is likely. Having committed an unauthorized access, the defendant is held strictly liable for the unpredictable victim reactions that follow.

One response might be that the threat of severe punishment made possible by a strict liability standard may deter computer crimes. The government brings only about 100 CFAA prosecutions per year,[93]

---

89 *See id.* at 15–16.

90 *See id.* at 29; *see also* U.S. SENTENCING GUIDELINES MANUAL § 5A (U.S. SENTENCING COMM'N 2014).

91 *See* U.S. SENTENCING GUIDELINES MANUAL § 5A.

92 *See* U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 (U.S. SENTENCING COMM'N 2015).

93 A query of the Bureau of Justice Statistics database reveals the following number of CFAA prosecutions per year from 2012 going back to 2004: 104, 108, 93, 149, 123, 102, 124, 114, and 94, respectively. *See Federal Criminal Case Processing Statistics*, BUREAU JUST. STATS.,

suggesting that the CFAA is woefully underenforced. Perhaps risk of a severe sentence for even a relatively minor offense serves a useful deterrent role. One argument for the felony murder rule is that its strict liability approach might make a wrongdoer think twice before committing a felony; the risk of murder liability for an accidental or even random death during the felony might cause the wrongdoer not to commit the crime in the first place.[94] Maybe hackers make the same calculation.

This argument is unpersuasive for the same reason it fails to persuade in the felony murder context. First, it ignores the necessary retributive limits on punishment.[95] Deterrence is not everything; punishments should not exceed what is just in that case.[96] Second, even if deterrence is the sole guide, the need to deter harm through higher punishments should be imposed broadly *ex ante* based on the expected harm of the wrongful act. The severity of punishments should not depend heavily on the happenstance of whether conduct triggered harms in that case judged *ex post*.

From a retributive perspective, relying on the loss chart for victim-response losses is similarly problematic. The moral culpability of the act lies in the act itself, not in the unpredictable cost of victim reaction. Under the loss chart approach, the length of the jail sentence is determined by fortuities such as how many hours the victim's employees spent responding to the crime and their hourly rates. Such numbers are sufficiently unpredictable for computer trespass crimes that they are not likely to match the culpability of the defendant's act.

A case I observed when I was at the Justice Department demonstrates the problem. The victim suffered a wide-scale CFAA offense directed against his website. In an initial interview with the victim, investigators asked him the questions directly relevant to the likely sentence. First, how many hours have you spent responding to the attacks? The answer: Lots and lots of hours. Next question: What is your hourly rate? According to the victim, he had no hourly rate. The website was his own, and he could not charge anyone for his time or even estimate what his rate might be. The investigation came to a

---

http://www.bjs.gov/fjsrc/ (under "Choose a Statistic" select "number of defendants in cases filed"; select years "2012" through "2004") (last visited Sept. 23, 2016).

94 *See, e.g.*, David Crump, *Reconsidering the Felony Murder Rule in Light of Modern Criticisms: Doesn't the Conclusion Depend upon the Particular Rule at Issue?*, 32 HARV. J. L. & PUB. POL'Y 1155, 1163 (2009).

95 *See* HERBERT L. PACKER, THE LIMITS OF THE CRIMINAL SANCTION 40 (1968).

96 *See id.*

halt. Under the section 2B1.1 loss chart, a victim with no hourly rate may have suffered no loss at all.

The current text of section 2B1.1 exacerbates this problem by removing the foreseeability requirement for victim-response losses in CFAA cases. The almost universal rule is that actual losses in section 2B1.1 only count if they are foreseeable.[97] The foreseeability requirement ensures that defendants are not punished for random or unpredictable losses. But this rule is suspended in just a single situation: "[i]n the case of an offense under 18 U.S.C. § 1030," victim response losses are included even if they are unforeseeable.[98]

It is not entirely clear why this language was added. My best guess is that the Sentencing Commission worried that judges wouldn't appreciate the foreseeability of victim-response losses in CFAA cases. To ensure that judges would consider those foreseeable losses, the Sentencing Commission made all victim-response losses count even if they were entirely *un*foreseeable. Whatever the reason, the inclusion of unforeseeable losses makes CFAA sentences even further removed from what the traditional justifications of punishment would require.

One bright spot under the current Guidelines is that unforeseeable victim-response losses must be reasonable to be included.[99] If a victim spends too much time responding to an intrusion, or otherwise runs up victim-response costs in an unreasonable way, the sentencing judge is supposed to cut down the victim-response losses to reasonable costs.[100] Although this can limit victim-response losses in theory, there are two reasons to doubt that it provides the needed limit in practice.

First, the lack of standards about what is an appropriate victim response makes it difficult to distinguish reasonable and unreasonable responses. As noted earlier, different victims will respond to intrusions differently.[101] Some will invest a great deal of time and others will not. The lack of standards can make it hard to say that a particular victim response is unreasonable as a matter of law. Second, even when judges do have a general sense of what makes a response unreasonable, they may be cautious about making judgments in a particular case. Judges are not computer security experts. They may feel out of

---

97 U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 cmt. n.3(A) (U.S. SENTENCING COMM'N 2015).

98 *Id.*

99 *Id.* ("Actual loss includes . . . any reasonable cost to any victim . . . .").

100 *See, e.g.*, United States v. Stratman, No. 4:13-CR-3075, 2014 WL 3109805, at *1–2 (D. Neb. July 8, 2014).

101 *See supra* Section II.C.

their element making judgments about whether a particular amount of time or cost was reasonable. For that reason, the limit of reasonableness may amount to less in practice than it might be in theory. I am aware of only one federal case in which a court carefully considered whether victim-response losses were reasonable and limited the losses accordingly.[102]

E. The Improper Use of Sophisticated Means and Special Skills Enhancements

A second flaw with the existing Guidelines in CFAA cases is widespread judicial reliance on the "sophisticated means" adjustment of section 2B1.1(b)(10)(C) and the "special skills" adjustment of section 3B1.3. Courts have routinely used these enhancements to make punishments more severe in CFAA cases.[103] This routine use is mostly unwarranted.

The sophisticated means enhancement provides a two-level enhancement in economic crimes cases when the crime is committed using sophisticated means, defined as "especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense."[104] For example, "[c]onduct such as hiding assets or transactions, or both, through the use of fictitious entities, corporate shells, or offshore financial accounts also ordinarily indicates sophisticated means."[105]

The special skills enhancement is somewhat similar, but it applies generally rather than only in economic crimes cases. It increases an offense level by two levels if the defendant used a special skill "in a manner that significantly facilitated the Sentencing Commission or concealment of the offense," with the caveat that the increase should not be applied if the "skill is included in the base offense level or specific offense characteristic."[106] "Special skill" is in turn defined as "a skill not possessed by members of the general public and usually requiring substantial education, training or licensing. Examples would

---

102 *See Stratman*, 2014 WL 3109805, at *1–2.

103 *See, e.g.*, Transcript of Proceedings: Sentence at 15–16, United States v. Auernheimer, No. 11-cr-470 (SDW), 2012 WL 5389142 (D.N.J. Mar. 18, 2013).

104 U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 cmt. n.9(B). *See generally* Miriam H. Baer, *Unsophisticated Sentencing*, 61 WAYNE L. REV. 61 (2015) (discussing "the 'sophisticated means' enhancement for fraud offenses under Section 2B1.1(b)(10)(C)").

105 U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 cmt. n.9(B).

106 *Id.* § 3B1.3.

include pilots, lawyers, doctors, accountants, chemists, and demolition experts."[107]

Although data is sparse, courts appear to have widely used both enhancements in run-of-the-mill CFAA cases. Even simple computer use has been deemed a sophisticated means. For example, in *United States v. Musacchio*,[108] the defendant asked a system administrator at his former company to read the email of current employees and to forward him relevant messages.[109] The Fifth Circuit affirmed the trial court's application of the sophisticated means enhancement at sentencing.[110] According to the Fifth Circuit, reading another person's email "concealed [the defendant's] identity"[111] and forwarding emails "using webmail accounts"[112] was an "attempt to avoid leaving records."[113] Although the court acknowledged that "many individuals familiar with computers likely could have developed a similar process,"[114] it concluded that reading and forwarding email was sufficiently sophisticated to deserve extra punishment.[115] It appears that, at least to some courts, figuring out how to commit a CFAA violation is inherently sophisticated.

Courts have applied the special skills enhancement widely in CFAA cases, as well.[116] For example, in *United States v. Shuster*,[117] a defendant pled guilty to violating the CFAA after he sent a denial-of-service attack and changed work account passwords.[118] After receiving the special skills enhancement, the defendant sought postconviction relief on the ground that his lawyer was ineffective because of his failure to explain that any person could have mounted the same attack.[119] The court disagreed on the ground that how to commit the CFAA violation "did not involve knowledge within the understanding

---

107 *Id.* § 3B1.3 cmt. n.4.

108 United States v. Musacchio, 590 F. App'x. 359 (5th Cir. 2014), *aff'd on other grounds*, 136 S. Ct. 709 (2016).

109 *Id.* at 361, 366.

110 *See id.* at 366.

111 *Id.*

112 *Id.*

113 *Id.*

114 *Id.*

115 *Id.* at 366–67.

116 *See, e.g.*, United States v. O'Brien, 435 F.3d 36, 42 (1st Cir. 2006); United States v. Lee, 296 F.3d 792, 798–99 (9th Cir. 2002); United States v. Petersen, 98 F.3d 502, 507–08 (9th Cir. 1996).

117 United States v. Schuster, Nos. 04-CR-00175-C, 3:07-cv-00614-bbc, 2008 WL 4449972 (W.D. Wis. Jan. 31, 2008).

118 *Id.* at *1.

119 *Id.* at *3.

of the ordinary lay person" or "matters of common knowledge."[120] By that standard, most CFAA crimes require special skills.

These enhancements are hard to justify. The sophisticated means enhancement makes sense in fraud cases but has no obvious justification in trespass cases. In a fraud case, a defendant who goes to great lengths to keep the fraud hidden can commit a wider-scale offense.[121] Most CFAA prosecutions, however, involve trespass rather than fraud.[122] It is less clear why concealing a trespass makes it more culpable or worthy of deterrence. To the extent the difficulty of investigating CFAA crimes should be a ground for extra punishment, it is likely already accounted for by the victim-loss consideration in the section 2B1.1 loss chart.[123] Difficulty catching a criminal will generally mean more time investigating the offense. Under section 2B1.1, that already translates into higher economic losses and a greater punishment.

Similarly, it is unclear why CFAA defendants should be punished more for using computer expertise under the special skills enhancement. Committing a CFAA offense often requires expertise.[124] It seems odd to punish defendants for committing the crime and then to punish them more for having the expertise needed to commit it.[125] More broadly, even if some computer skills are "special," they do not seem special in the way ordinarily recognized in section 3B1.3.[126] The purpose of section 3B1.3 is to recognize the special harms when defendants take advantage of society's trust in certain professions and positions to give them less oversight.[127] The possession of special skills means less oversight by others and more trust; the abuse of those skills is an abuse of that trust.[128] That rationale has little application to computer skills. Society does not normally trust people who know how to

---

120 *Id.*

121 *See* Baer, *supra* note 104, at 73–74, 78–80.

122 *See supra* Section II.B.

123 *See supra* Section II.A.

124 *See, e.g.*, United States v. Auernheimer, 748 F.3d 525, 530–31 (3d Cir. 2014).

125 *See* United States v. Young, 932 F.2d 1510, 1513 (D.C. Cir. 1991) ("[T]he Sentencing Commission assumed that the defendant knows how to commit the offense in the first place and that he uses a 'special skill' to make it *easier* to commit the crime. Thus, the 'special skill' necessary to justify a § 3B1.3 enhancement must be more than the mere ability to commit the offense . . . .").

126 *See id.* at 1514–15.

127 *See* U.S. SENTENCING GUIDELINES MANUAL § 3B1.3 cmt. n.1 (U.S. SENTENCING COMM'N 2015).

128 *See id.*

hack into computers.[129] People who develop those skills generally do so on their own, not with the blessing of, or a special license from, the public.[130]

III. A New Approach to CFAA Sentencing

The Sentencing Commission should revisit CFAA sentencing. CFAA cases should be treated in two different ways. First, CFAA crimes that are really about trespass—cases brought under § 1030(a)(2)–(3) and (5)(B)–(C)—should be punished under a new guideline. CFAA offenses that still fit within section 2B1.1, the § 1030(a)(4) crimes and § 1030(a)(5)(A) offenses, should be punished under an amended section 2B1.1. Second, the Sentencing Commission should narrow the use of the sophisticated means and special skills enhancements in CFAA cases.

A. A New Guideline for Computer Trespass Offenses—§ 1030(a)(2)–(3) and (5)(B)–(C)

The major CFAA crimes found in § 1030(a)(2)–(5) are divided into two types. Several provisions—§ 1030(a)(2)–(3) and (5)(B)–(C)—are, at their core, trespass offenses in which the primary wrong is the privacy violation of the unauthorized access.[131] Sentencing recommendations under these sections should be made under a new guideline appropriate for computer trespass offenses. The new guideline should still consider consequential losses, but it should not add as many levels as the section 2B1.1 loss chart.

For example, CFAA trespass guidelines might treat consequential losses as follows:

> If the offense caused losses of—
> (A) at least $10,000 but less than $20,000, increase by 2 levels;
> (B) at least $20,000 but less than $50,000, increase by 3 levels;
> (C) at least $50,000 but less than $150,000, increase by 4 levels; and
> (D) more than $150,000 increase by 5 levels.

---

129 *See* Michael Bywater, *Hackers Aren't the New Mafia—They Aren't Trustworthy Enough*, Week (July 20, 2012), http://www.theweek.co.uk/books/48069/hackers-arent-new-mafia-they-arent-trustworthy-enough.

130 Taylor Armerding, *Self-Taught Hackers Rule*, CSO (Apr. 23, 2014, 6:29 AM), http://www.csoonline.com/article/2146363/security-leadership/self-taught-hackers-rule.html.

131 *See* 18 U.S.C. § 1030(a)(2)–(3), (5)(B)–(C) (2012).

A new CFAA trespass guideline could also add adjustments for the kinds of factors that are recognized as particularly blameworthy both under section 2B1.1 and under the felony provisions of the CFAA. Examples could include intent to profit; conduct in furtherance of a criminal scheme; intent to obtain personal information; distribution of personal information; and damage to critical infrastructure.

The new guideline could also include an increase in levels for obtaining economically valuable information. The CFAA makes this a felony instead of a misdemeanor when the value of the information exceeds $5000, but the existing Guidelines leave unclear how this should be treated.[132] If the information is worth $5000, does that mean that the obtaining of the information is a $5000 loss? The existing Guidelines offer no clear answer.

A new guideline would be appropriate for computer trespass offenses because no existing guideline is appropriate. Notably, the current Guidelines do have a trespass section, section 2B2.3, which is used to sentence defendants in the rare case of a simple trespass crime under 18 U.S.C. § 1030(a)(3).[133] This provision is problematic, however, because, among other things, it also uses the loss chart of section 2B1.1 for any CFAA loses that exceed $5000.[134] The better approach would be to start from scratch with a new guideline section that is directly tailored to the harms and context of CFAA trespass crimes.

B. Amend Section 2B1.1 for Computer Fraud and Intentional Computer Damage—§ 1030(a)(4)–(5)(A)

The second set of core CFAA offenses consists of fraud and intentional damage cases brought under § 1030(a)(4)–(5)(A). In these cases, the broad framework of section 2B1.1 is mostly appropriate because economic loss is intentional. Defendants in these cases either committed intentional fraud schemes under § 1030(a)(4) or intentionally damaged victim computers under § 1030(a)(5)(A). Economic loss is at the core of these offenses much like it would be for a traditional case of fraud or property damage. Nonetheless, a few changes to sec-

---

132 *Id.* § 1030(c); *see also* U.S. SENTENCING GUIDELINES MANUAL § 2B1.1.

133 U.S. SENTENCING GUIDELINES MANUAL § 2B2.3.

134 *See id.* § 2B2.3(b)(3) ("If (A) the offense involved invasion of a protected computer; and (B) the loss resulting from the invasion (i) exceeded $2,500 but did not exceed $6,500, increase by 1 level; or (ii) exceeded $6,500, increase by the number of levels from the table in § 2B1.1 (Theft, Property Destruction, and Fraud) corresponding to that amount.").

tion 2B1.1 should be made to better tailor sentencing of these CFAA offenses.

First, the losses that are treated under the section 2B1.1 loss chart should be limited to losses that are part of the fraud, not mere victim-response losses. Victim-response losses should be treated under a separate adjustment mirroring the approach to victim-response losses in the separate computer trespass guideline.[135] If a defendant hacks into a computer and uses that access to commit a $50,000 fraud, which then leads to $50,000 in victim-response losses, the two losses should be treated differently: the $50,000 in fraud loss should be treated under the loss chart, and the $50,000 in victim-response loss should be treated under the separate provision for victim-response losses.

Second, the separate adjustments for CFAA crimes in the current section 2B1.1 can mostly be moved into the new computer trespass guideline. The "fraud plus" approach of the current section 2B1.1[136] should be divided into two approaches, with the "fraud" framework applied in section 2B1.1 for CFAA offenses that are fraud or damage crimes and the "plus" framework moved into the separate guideline for computer trespass crimes.

C. Rethink Special Skills and Sophisticated Means Enhancements

A final change to the Guidelines should be limits on the use of sophisticated means and special skills enhancements in CFAA cases. Because CFAA trespass offenses would be sentenced under a new section, the sophisticated means provision of section 2B1.1 would not apply to those crimes. The Sentencing Commission should also update the current sophisticated means guidance to ensure that it does not apply to routine computer use.[137] Finally, section 3B1.3 should be amended to clarify that even expert computer skills are ordinarily not "special skills."

Conclusion

The Sentencing Commission should create a new guideline for CFAA trespass offenses and amend the existing guideline for CFAA fraud and damage offenses. By enacting these changes, it could restore common sense to CFAA sentencing and ensure that sentences better measure the seriousness of CFAA offenses. The Sentencing

---

135 *See supra* Section III.A.

136 *See supra* Section I.C.

137 *See* Baer, *supra* note 104, at 66 ("[M]ere amateurs can easily undertake the conduct that society previously deemed so 'sophisticated.'").

Commission began on the wrong track in 1988 when it assumed that CFAA crimes were a form of fraud. Over a quarter of a century later, it is time to correct that error and take a better path.