FEDERAL PUBLIC DEFENDER
District of Arizona
850 West Adams Street, Suite 201
PHOENIX, ARIZONA 85007

JON M. SANDS
Federal Public Defender

(602) 382-2700
1-800-758-7053
(FAX) 382-2800

March 27, 2009

Honorable Ricardo H. Hinojosa
Acting Chair
United States Sentencing Commission
One Columbus Circle, N.E.
Suite 2-500, South Lobby
Washington, D.C. 20002-8002

Re: Comments on ID Theft and Computer Crimes

Dear Judge Hinojosa:

With this letter, we provide comments on behalf of the Federal Public and Community Defenders on the proposed amendments and issues for comment relating to the directives set forth in § 209 of the Identity Theft Enforcement and Restitution Act of 2008, Pub. L. 110-326 (Sept. 26, 2008), and other issues related to identity theft and computer crimes, that were published in the Federal Register on January 27, 2009.[1] At the public hearing on March 17, 2009, we submitted written testimony on these matters. A copy of that written testimony, which includes the written comment by Martin Richey submitted on December 8, 2008, is attached and incorporated as part of this public comment.

We do not reiterate here our important arguments regarding deterrence, recidivism, and complexity. We address a few specific issues that were discussed at the public hearing.

A. The Commission Should Not Amend the Guidelines to Account for Individuals Who Do Not Suffer Monetary Loss in Identity Theft Cases.

As we stated in our written testimony, the Commission should not expand the definition of victim under USSG § 2B1.1(b)(2) to account for individuals who did not suffer monetary loss or who were fully reimbursed for their monetary losses, either on the basis of privacy concerns or on time spent resolving problems.

[1] *See* 74 Fed. Reg. 4,802, 4,803-10 (Jan. 27, 2009).

The available data does not show that a substantial number of individuals suffer significant non-monetary harm. Many individuals are not even aware that their identifying information has been misused. According to a survey conducted by the Federal Trade Commission, of those who are aware of the misuse, only about a quarter report, as a primary concern, the emotional toll resulting from an invasion of privacy.[2] A substantial proportion (30%) of those individuals who are aware that their identifying information was misused spent *an hour or less* resolving problems associated with the misuse of their identifying information, with the median reporting only spending four hours.[3] Only ten percent reported spending 55 hours or more resolving problems.[4]

At the hearing, the Department of Justice's *Ex Officio* asked Eric Handy, the representative at the hearing from the Identity Theft Resource Center, if that organization has any empirical evidence indicating the number of individuals suffering non-monetary harm in identity theft cases. Although Mr. Handy indicated that the organization studies that question every year, neither he nor the organization provided evidence that contradicted the information reported by the Federal Trade Commission.

The varying, and often very little, amount of time spent correcting problems caused by identify theft shows why the number of victims alone is a poor measure of harm and why the current invited upward departure provides a more appropriate way of accounting for substantial non-monetary harm. The Commission itself recognized in 1999 that reliance on the number of victims alone "can result in either overstating or understating the harm."[5] To account for circumstances in which the guideline "substantially understates the seriousness of the offense," USSG § 2B1.1, comment. (n.19(A)), the Commission provided for an upward departure where the offense "caused or risked substantial non-monetary harm," such as "psychological harm, or severe emotional trauma or resulted in a substantial invasion of privacy interest," *id.* comment. (n.19(A)(ii)).

Absent data indicating that courts are frequently departing upward to account for those atypical individuals who suffer an unusual amount of non-monetary harm, the Commission should not add unnecessary complexity to § 2B1.1 or increase penalties in a manner that may overstate the harm in many cases.

[2] Federal Trade Commission, *2006 Identity Theft Report*, at 52-53 & fig. 21 (Nov. 2007).

[3] *Id.* at 5-6 & tbl. 2.

[4] *Id.*

[5] USSC, *Identity Theft Final Report*, at 26 (Dec. 15, 1999).

B. Any Amendment to Account for Non-Monetary Harm in Identity Theft Cases Should Be Narrowly Tailored.

We recognize that the Commission may view this issue in identity theft cases as one that requires action in the form of an amendment to § 2B1.1, regardless of whether courts are or are not frequently departing upward. Although the Commission has not published a proposed amendment, we understand that it may act in some manner, perhaps by amending the definition of "loss" at Application Note 3 to count as "victims" those who do not suffer pecuniary harm but who suffer some other form of harm, or by amending the victim table at subsection (b)(2) to capture those individuals whose personal information was misused but who did not ultimately suffer any monetary loss. We continue to believe that such change is unnecessary, and we object to the promulgation of unpublished amendments. However, we offer the following thoughts regarding the scope of any such change.

First, any enhancement should be carefully circumscribed so that it captures only aggravated cases. In our written testimony, we proposed a special rule that would add a one-level enhancement if any person, otherwise not counted as a victim under § 2B1.1(b)(2), reasonably spent 50 hours or more resolving financial problems resulting from the misuse of the identifying information. This would limit the enhancement to capture harm not already captured by the loss table and to count only those individuals who experienced *aggravated* non-monetary harms as opposed to those non-monetary harms intrinsic to identity theft offenses.

If the Commission chooses to focus instead on the number of individuals who suffer non-monetary harm rather than the extent of the non-monetary harm in a particular case, it should not create a rule that would count each person at the same *rate* as a victim who suffered monetary harm. Instead, the Commission might add a special rule for identity theft offenses that adds a unitary enhancement when the offense involves a very large number of victims who suffer non-monetary harm, leaving the departure provision at Application Note 19 to account for those situations involving individuals who suffer truly unusual non-monetary harm. For example, the Commission might create a special rule for identity theft cases to add one level if the offense involved more than a certain large number of individuals who are not otherwise counted as victims under subsection (b)(2) but whose personal information was misused. Depending on the Commission's data regarding the typical case, the number of individuals should be high enough so that it will limit the enhancement to those identity theft cases in which the number of individuals whose identifying information was actually misused represents the *aggravated* case.

A useful analogy might be drawn from the mass-marketing enhancement at subsection (b)(2)(A)(ii). That two-level increase functions as an alternative method for accounting for large numbers of individuals who may have been affected by an offense but who have not necessarily suffered monetary harm. In 2004, when the Commission broadened that enhancement to apply automatically to conduct described in 18 U.S.C. §

1037 (involving email spam), regardless of whether the person was convicted of § 1037, it explained that it was responding to Congress's concern regarding "offenses that are facilitated by sending large volumes of electronic mail." USSG, App. C, Amend. No. 665 (Nov. 1, 2004). For identity theft offenses involving large volumes of small harms or harms difficult or impossible to measure, similar reasoning might apply.

At least one court has recognized that estimating non-monetary or emotional harm may not be an appropriate measure of harm in cases involving large numbers of affected individuals who experience differing levels of subjective, non-monetary harm. In a case involving a massive email spam operation prosecuted under 18 U.S.C. § 1037, the government asked the court to apply the six-level enhancement for "over 250 victims" under USSG § 2B1.1(b)(2)(C) based on its theory that "hundreds of millions, perhaps billions," of people received the spam, and each had to spend some time deleting the spam or resolving problems resulting from the spam. *See* Gov't Sentencing Mem., at 16, *United States v. Soloway*, No. CR07-187MJP (July 22, 2008). Only sixty-one individuals submitted victim impact statements, however, with some relying on varying methods of calculating their non-monetary or emotional harms.

Regarding the losses claimed by the victims, the judge declined to calculate loss based on individual victims' lost time or emotional damage, stating: "I would never be able to calculate what the loss was. It would be impossible. Because there are so many people and there are so many shades of grey amongst them." Tr. of Sentencing Proceedings, at 3, *United States v. Soloway*, No. CR07-187MJP (July 22, 2008). For similar reasons, the judge declined to apply the enhancement for more than 250 victims, finding that the alternative two-level increase under subsection (b)(2)(A)(ii) for offenses involving mass-marketing was more appropriate in such a case. *Id.* at 5. She explained:

> [C]ounting victims is a very difficult task . . ., trying to define who is truly a victim and who is not. We will have millions of people out there who are harmed but who didn't know where to complain, we have people who complained to entities that couldn't do anything about it. . . .
>
> But the guidelines are also helpful to us there, because they say when this is a mass market event, then you count two points. . . . I can't count victims one-by-one.

Id.

As recognized by the judge there, the alternative mass-marketing enhancement indicates that the Commission concluded that a uniform increase in the offense level is appropriate regardless of whether an offense involved a hundred, a thousand, or a billion emails. Just as in cases involving email spam, counting untold numbers of victims in offenses involving identity theft would risk imprecise and varying measures of harm and could easily overstate the harm in cases involving large numbers of individuals whose information was used. Our proposals would limit the enhancement to obviate these risks.

C. The Commission Should Not Disaggregate Intent to Cause Damage and Intent to Obtain Personal Information in 18 U.S.C. § 1030 Cases.

In our written testimony, we stated that the Commission should not disaggregate a defendant's intent to cause damage and intent to obtain personal information so that they are considered separately from the other factors set forth in § 2B1.1(b)(15) related to offenses under 18 U.S.C. § 1030. We are not aware of any new data indicating that the Commission's stated rationale for structuring the enhancements in an incremental manner to punish incrementally more serious offenses is no longer supported.

In its written testimony for the hearing on March 17th, the Department of Justice asserts that the provision is not functioning in its intended manner, and that it "mandates the same sentence for strikingly dissimilar conduct." As examples, the Department compared the defendant who intended to obtain personal information from a grocery store with a defendant who intended to obtain such information from a "critical infrastructure computer," and a defendant who intentionally damaged a military computer with one who intentionally damaged a computer in someone's home. According to the Department, the first offense in each example is more serious than the second.

Setting aside the fact that the guidelines no longer "mandate" sentences, the Department's arguments depend on its assumption that § 1030 offenses involving government computers or computers used to operate or maintain critical infrastructures are *always* more serious than offenses involving other computers. Its proposed amendment would increase from two to four levels the enhancement for the individual who intended to obtain personal information from a critical infrastructure computer (as opposed to a grocery store, which would continue to get a two level enhancement), and increase from four to six levels the enhancement for the person who intended to damage a military computer (as opposed to a personal computer not part of any critical infrastructure, which would continue to get a four-level enhancement). In addition, the enhancements for intent to obtain personal information and intentional damage to a protected computer would apply cumulatively to each other and to the enhancement for computers involving a critical infrastructure.

While the Department makes a blanket assertion that critical infrastructure computers "typically contain far more sensitive information, such as medical records and classified information" and that "obtaining personal information from these types of computers clearly warrants more severe punishment," it offers no evidence to support that view. The Commission defines "critical infrastructure" as "systems and assets vital to national defense, economic security, public health or safety or any combination of those matters." USSG § 2B1.1, comment. (n.13(A)). A critical infrastructure can be either privately or publicly owned, and examples include not only systems that may maintain medical records or classified information, but also gas and oil production, storage and delivery systems, water supply systems, telecommunications networks,

electrical power delivery systems, financing and banking systems, and highway and mass transit systems, including airlines and airports. *Id*. Obviously, not all critical infrastructure computers contain "more sensitive information, such as medical records and classified information," as the Department asserts.

Further, all personal information is potentially "sensitive," which is why the guidelines already have a two-level increase to account for the intent to obtain personal information. The Commission defines "personal information" as "sensitive or private information (including such information in the possession of a third party), including (i) medical records; (ii) wills, (iii) diaries, (iv) private correspondence, including email; (v) financial records; (vi) photographs of a sensitive or private nature; or (vii) similar information." USSG § 2B1.1, comment. (n.(13(A)). Nothing indicates that some of this information is more sensitive or private than the others. Many people keep highly sensitive information on their personal computers, such as diaries and photographs, which may be far more sensitive than any personal information kept by an electric company or airline. And with the advent of electronic records, many lawyers, doctors, and others keep information on many clients on laptops and other personal computers.

For those cases in which the two-level enhancement for intent to obtain personal information does not adequately capture the seriousness of the offense or the sensitivity of the information, Application Note 19 provides for upward departure if the "offense caused or risked a substantial non-monetary harm," such as "invasion of privacy interest (through, for example, the theft of personal information such as medical, educational, or financial records"). USSG § 2B1.1, comment. (n.19(A)(ii)). It also provides for upward departure for offenses involving stolen information from a protected computer if "the defendant sought the stolen information to further a broader criminal purpose." *Id.* comment. (n.19(A)(v)).

In any event, even if the Commission concludes that intent to obtain personal information from a critical infrastructure computer is more serious than intent to obtain personal information from a personal computer, and that the difference is not adequately reflected by the current structure of § 2B1.1(b)(15)(a), the solution is not necessarily to *increase* the range for intent to obtain personal information from a critical infrastructure computer, but could be to *decrease* the range for offenses involving intent to obtain personal information from a computer that is not used to maintain or operate a critical infrastructure.

With respect to intentional damage under 18 U.S.C. § 1030(a)(5)(A), the Department simply states, again without supporting evidence, that the social harm is greater when a defendant intentionally damages a critical infrastructure computer, as opposed to a personal computer. However, it does not explain why this is necessarily true. To the extent that Congress has criminalized conduct involving intentional damage to a personal computer that does not affect a financial institution or the United States Government, it did not distinguish between those computers and other protected computers for penalty purposes. The aim of § 1030(a)(5)(A) is to punish intentional

damage to any "protected computer." The focus of the current enhancement is to punish the intent to damage, regardless of the type of protected computer. We are unaware of any data indicating how many offenses under § 1030(a)(5)(A) involve personal computers versus military computers, or how courts are treating these two types of offenses. The Department's proposal adds unnecessary complexity to a guideline whose "defects," as far as we know, have not been made apparent by judicial feedback in the form of departures or variances.

As with intent to obtain personal information, even if the Commission concludes that intentional damage to a military computer is more serious than intentional damage to a personal computer, the solution should not necessarily mean that the guidelines must be amended to *increase* the range for damage to military computers. The Commission could *decrease* the range for offenses involving intentional damage only to a personal computer to achieve the desired result.

As always, we very much appreciate the opportunity to submit comments on the proposed amendments. We look forward to continue working with the Commission on these and other matters.

Very truly yours,

JON M. SANDS
Federal Public Defender, District of Arizona
Chair, Federal Defender Sentencing Guidelines Committee

cc: Hon. Ruben Castillo, Vice Chair
Hon. William K. Sessions III, Vice Chair
Commissioner William B. Carr, Jr.
Commissioner Dabney Friedrich
Commissioner Beryl A. Howell
Commissioner *Ex Officio* Edward F. Reilly, Jr.
Commissioner *Ex Officio* Jonathan Wroblewski
Ken Cohen, General Counsel
Judith M. Sheon, Staff Director
Kathleen Grilli
Michael Courlander, Public Affairs Officer

Testimony of Jennifer N. Coffin
Staff Attorney
Sentencing Resource Counsel
On Behalf of the Federal Public and Community Defenders
Before the United States Sentencing Commission
Public Hearing on Proposed Amendments for 2009
March 17, 2009

Thank you for the opportunity to testify on behalf of the Federal Public and Community Defenders regarding the Commission's requests for comment regarding offenses involving computer crimes and the misuse of identifying information.

I. OVERVIEW

With the Identity Theft Restitution and Enforcement Act of 2008, Pub. L. 110-326 (Sept. 26, 2008) (the "Act"), Congress amended 18 U.S.C. § 1030 in order to strengthen the tools available for prosecuting offenses involving an individual's identifying information and computer crime.[1] These amendments, among other things, "ensur[ed] jurisdiction" over the "theft of sensitive identity information," guaranteed the use of "full interstate and foreign commerce power," and provided for forfeiture of property used to commit an offense under that section. *Id.* §§ 203, 207, 208. Congress also amended 18 U.S.C. § 3663(b) to allow for restitution to victims of identity theft (18 U.S.C. §§ 1028(a)(7), 1028A) for the monetary value of time spent remediating the harm resulting from the offense.

Congress did not increase penalties for computer offenses or for offenses relating to identity theft. It directed the Commission to "review" the guidelines and policy statements applicable to convictions under 18 U.S.C. §§ 1028, 1028A, 1030, 2511, and 2701 "in order to reflect the intent of Congress that such penalties be increased in comparison to those currently provided by such guidelines and policy statements," *id.* § 209(a), and in determining "the appropriate sentence for the crimes enumerated," to consider "the extent to which the guidelines and policy statements may or may not account for" a set of thirteen factors "in order to create an effective deterrent to computer crime and the theft or misuse of personally identifiable data." *Id.* § 209(b).

Eight of these factors are virtually identical to the factors studied by the Commission in 2002, as directed in § 225(b)(2) of the Cyber Security Enhancement Act of 2002, Pub. L. No.107-296. The Commission responded to those factors, particularly with respect to offenses under 18 U.S.C. § 1030, and explained its actions in a report to Congress.[2] Thus, not only has the Commission already considered many of the factors in

[1] *See* Statement of Senator Patrick Leahy, Chairman, Committee on the Judiciary, On Passage of the Former Vice President Protection Act of 2008, H.R. 5938 (Sept. 15, 2008), available at http://leahy.senate.gov/press/200809/091508b.html.

[2] *See* USSG, App. C, Amend. 654 (Nov. 1, 2003); USSC, *Increased Penalties for Cyber Security Offenses* (May 2003) "(Cyber Crimes Report").

§ 209(b) of the Identity Theft Enforcement and Restitution Act of 2008, it appears that Congress may not even have been aware of the Commission's actions when it repeated those factors in this Act.

On November 20, 2008, J. Martin Richey, Assistant Federal Public Defender, spoke on behalf of the Federal Defenders at the Commission's briefing regarding this directive. On December 8, 2008, Mr. Richey followed up with written comments (which are attached as Appendix A), setting forth our view that, absent evidence that the guidelines in their present form do not adequately address the concerns raised in the directive and its predecessor, there is no need for further action.[3] He also addressed in some detail several of the thirteen factors, articulated a number of mitigating factors that might constitute grounds for downward departure in identity theft or computer crimes cases (as requested by Commissioner Howell), and asked the Commission to share any data analyzed as part of its review of the guidelines as directed by Congress.

The Commission has now proposed amendments to USSG §§ 2B1.1, 2H3.1, and 3B1.1 and published several issues for comment regarding Congress's directive and "other related issues." The Commission does not suggest that its data analysis revealed that judges have found these guidelines wanting when considering the purposes of sentencing under 18 U.S.C. § 3553(a)(2). Yet, without exception, the proposed amendments would increase the Commission's recommended punishments through expanded definitions, new specific offense characteristics, or broadened grounds for upward departure. In addition, these proposed changes would add yet more complexity to the guidelines at a time when all agree that they are in dire need of simplification. At the same time, there is no indication that the Commission has found, based on empirical data, that the proposed changes would "create an ***effective deterrent*** to computer crime and theft or misuse of personally identifiable information," as directed by Congress in § 209(b) (emphasis added).

We urge the Commission first to consider the substantial evidence that increasing guideline ranges would not be an effective deterrent to computer crime or theft or misuse of personally identifying information. It is the certainty of punishment (***i.e.***, a high risk of being caught and prosecuted), rather than the severity of punishment, that deters crime. Further, the offenders at whom the Act is aimed present a low risk of committing future crimes, thus indicating that no increase is necessary for the purpose of specific deterrence or protection against further crimes of the defendant.

We also urge the Commission not to add further unnecessary complexity to the guidelines. Section 2B1.1 is far too complex already, wasting time and resources on hypertechnical disputes unrelated to the purposes of sentencing, and is more than adequate to account for the factors under consideration.

---

[3] *See* Letter from J. Martin Richey to Hon. Ricardo Hinojosa, *Re: Public Comment on Commission action in response to Pub. L. 110-326, § 209 (a directive relating to identity theft and computer crimes)*, at 1 (Dec. 8, 2008).

Finally, we address the factors listed in the directive and one that is not, focusing primarily on those regarding which the Commission has proposed amendments, or asked for comment and indicated a particular interest in our feedback.

Overall, we urge the Commission not to accede to the misguided view that it can or should attempt to stop identity theft by increasing guideline ranges. As Senator Leahy, the author of the Act, recognized, higher penalties and broader jurisdiction over criminal offenses do not address identity theft "at its source," which is "lax data security and inadequate breach notification."[4] This is why, in most cases, banks and other businesses are civilly responsible for the loss.[5] While we do not suggest that identity thieves are not responsible for the harm they cause, the Commission should reject the assumption that increasing guideline ranges is an effective tool to stop it.

The Commission should also reject the assumption that guideline ranges should be increased to reflect non-pecuniary harm to victims. The vast majority of persons who experience misuse of their identifying information suffer little or no out-of-pocket monetary loss and spend a minimal amount of time resolving resulting problems. Going beyond measurable monetary harm would overstate the seriousness of the offense in most cases, while adding further difficulty to the sentencing process. Moreover, increasing a defendant's sentence — in some cases doubling the sentence — by expanding the definition of victim to include those who have not suffered monetary loss would do nothing to compensate victims. Restorative justice practices, through which victims and the defendant meet and agree on reparative measures, can actually repair non-pecuniary harms and discourage future crime in ways that increased prison terms cannot.

II. DETERRENCE, GENERAL AND SPECIFIC

A. Increasing penalties will not "create an effective deterrent."

By strengthening prosecutorial tools and expanding jurisdiction, Congress has increased the certainty that more offenders will be apprehended. It has directed the Commission to consider "the extent to which" the guidelines and policy statements account for the thirteen enumerated factors "in order to create an effective deterrent." The Department of Justice urges the Commission to assume that increasing penalties under §§ 2B1.1 and 2H3.1 will deter computer crime and identity theft. [6]

While many believe that the higher the sentence, the greater the effect in deterring others, current empirical research shows that while certainty has a deterrent effect,

---

[4] Statement of Senator Patrick Leahy, Chairman, Committee on the Judiciary, *On Senate Passage of the Identity Theft Enforcement and Restitution Act of 2007* (Nov. 15, 2007), available at http://leahy.senate.gov/press/200711/111607a.html.

[5] Federal Trade Commission, *2006 Identity Theft Report* at 6, n.5 (Nov. 2007) ("FTC Report").

[6] Letter from Michael M. Dubose, U.S. Dept. of Justice, to Hon. Ricardo H. Hinojosa, at 2 (Jan. 5, 2009) ("DOJ Letter").

"increases in severity of punishments do not yield significant (if any) marginal deterrent effects."[7] "Three National Academy of Science panels . . . reached that conclusion, as has every major survey of the evidence."[8] Typical of the findings on general deterrence are those of the Institute of Criminology at Cambridge University.[9] The report, commissioned by the British Home Office, examined penalties in the United States as well as several European countries. It examined the effects of changes to both the *certainty* and the *severity* of punishment. While significant correlations were found between the certainty of punishment and crime rates, the "correlations between sentence severity and crime rates . . . were not sufficient to achieve statistical significance."[10] The report concluded that "the studies reviewed do not provide a basis for inferring that increasing the severity of sentences generally is capable of enhancing deterrent effects."[11] Another review of this issue concluded: "There is generally no significant association between perceptions of punishment levels and actual levels . . . implying that increases in punishment levels do not routinely reduce crime through general deterrence mechanisms."[12]

In one of the best studies of specific deterrence, which involved federal white collar offenders (presumably the most rational of potential offenders) in the pre-guideline era, no difference in deterrence even between probation and imprisonment.[13] That is, offenders given terms of probation were no more likely to reoffend than those given prison sentences.

There are at least two good reasons why increasing guideline ranges for the nonviolent offenses at issue here will not reduce their incidence. First, potential offenders are not generally aware of the penalties for their prospective crimes. Second, "most offenders committing [crimes] naively but realistically, do not expect to be

---

[7] Michael Tonry, *Purposes and Functions of Sentencing*, 34 Crime & Just. 1, 28 (2006).

[8] *Id*.; *see also* Zvi D. Gabbay, *Exploring the Limits of the Restorative Justice Paradigm: Restorative Justice and White-Collar Crime*, 8 Cardozo J. Conflict Resol. 421, 447-48 (2007) ("[C]ertainty of punishment is empirically known to be a far better deterrent than its severity.").

[9] *See* Andrew von Hirsch, et al, *Criminal Deterrence and Sentence Severity: An Analysis of Recent Research* (1999). A summary of these findings is available at http://members.lycos.co.uk/lawnet/SENTENCE.PDF.

[10] *Id.* at 2.

[11] *Id.* at 1.

[12] Gary Kleck et al., *The Missing Link in General Deterrence Theory*, 43 Criminology 623 (2005).

[13] *See* David Weisburd et al., *Specific Deterrence in a Sample of Offenders Convicted of White-Collar Crimes*, 33 Criminology 587 (1995); *see also* Zvi D. Gabbay, *Exploring the Limits of the Restorative Justice Paradigm: Restorative Justice and White-Collar Crime*, 8 Cardozo J. Conflict Resol. 421, 448-49 (2007) ("[T]here is no decisive evidence to support the conclusion that harsh sentences actually have a general and specific deterrent effect on potential white-collar offenders.").

caught."[14] A recent survey estimated that only 26% of over 8 million people who discovered their identification information had been misused in 2005 reported the misuse to law enforcement.[15]

As the expert body charged by Congress with establishing sentencing policies and practices that "reflect, to the extent practicable, advancement in knowledge of human behavior as it relates to the criminal justice process," 28 U.S.C. § 994(b)(1)C), the Commission should resist perpetuating the erroneous assumption that increasing sentence severity will deter identity theft and computer crime.

B. The offenders at whom the directive is aimed present a low risk of recidivism.

To the extent that Congress has directed the Commission to study the factors listed at § 209(b) to determine whether increasing guideline ranges based on those factors will deter an individual offender from committing future crimes, the Commission should look to its data regarding the rate of recidivism for individuals convicted of offenses sentenced under USSG § 2B1.1.

In 2007, the majority of offenders (approximately 60%) sentenced in the primary offense categories of larceny, fraud and embezzlement were in Criminal History Category I.[16] For those convicted of computer offenses under 18 U.S.C. § 1030, the rate is even higher, at 78%.[17] Further, most violators of 18 U.S.C. § 1030 are well-educated, with 66% having completed at least some college education.

Commission data show that offenders in Criminal History I have a 13.8% rate of recidivism, the lowest across all criminal history categories.[18] College education is also associated with lower rates of recidivism, at 13.9% for some college education and 7.1% for a college degree in Criminal History Category I.[19]

These data show that increasing punishment is not necessary to prevent future crimes of the defendant.

---

[14] Tonry, ***supra*** note **7** at 29.

[15] FTC Report, at 50 & fig. 19.

[16] 2007 Sourcebook, tbl. 14.

[17] Cyber Crimes Report at 3.

[18] *See* USSC, *Measuring Recidivism: The Criminal History Computation of the Federal Sentencing Guidelines*, Ex. 2 (May 2004) (as compared to 24% for CHC II, 34.2% for CHC III, 44.6% for CHC IV, 51.6% for CHC V, and 55.2% for CHC IV).

[19] *Id.* at 12 & Ex. 10

C. Increasing sentences despite evidence that doing so will not "create an effective deterrent" reflects unsound policy.

Without empirical evidence demonstrating that an increase in sentence severity for these offenses would create a more effective deterrent to these crimes, the proposed amendments would unjustifiably expand Congress's directive beyond its intended scope. The Commission should exercise with confidence its core function of developing sentencing policy based on its own institutional expertise, tied to the purposes of sentencing, based on empirical evidence.

III. COMPLEXITY

The proposed amendments would add unnecessary complexity to the guidelines. Section 2B1.1 already spans over four full pages in the Guidelines Manual, followed by 17 pages of intricate commentary. As explained in our letter of December 8, 2008, the guidelines already adequately take into account the factors set forth in the directive at § 209(b). In response, the Department outlined several areas in which it seeks guideline increases. However, it does not provide or point to any empirical evidence indicating that judges have frequently had to sentence above the advisory guideline range in order to impose an appropriate sentence for offenses involving computers or misuse of identifying information.

At the recent hearing in Atlanta, Judge Conrad described the guidelines as having evolved into "a hypertechnical accounting practice, . . . focusing battles on sub-sections and application notes," ultimately disconnected from the purposes of sentencing.[20] The Commission has recognized that it is neither possible nor appropriate to capture every possible permutation of offense conduct, particularly when judges have not indicated that they are unable to account for relevant factors. *See* USSG, Ch. 1, pt. A, § (4)(b) ("it is difficult to prescribe a single set of guidelines that encompasses the vast range of human conduct."). Only when "the data permit" should the Commission conclude that a new factor is "empirically important," ***i.e.***, not already accounted for in the guideline and occurs frequently enough to be included as an enhancement to the offense level. ***See id.*** For those factors that occur infrequently, a court always has the discretion to depart or vary from the guideline range. ***Id.*** Absent a finding that the proposed changes are empirically necessary, the Commission should not add to the complexity of a guideline that is far too complex.

[20] Testimony of Robert J. Conrad, Jr., Chief United States District Judge, Western District of North Carolina, Regional Hearings on the Twenty-Fifth Anniversary of the Passage of the Sentencing Reform Act of 1984, View from the Bench, at 5 (Feb. 11, 2009).

IV. FACTORS ADDRESSED IN PROPOSED AMENDMENTS AND ISSUES FOR COMMENT

While we addressed to some extent the most salient factors of those enumerated in § 209(b) of the Act in our letter of December 8, 2008, we address all of the factors here (and one that is not listed in the directive) to a greater or lesser extent in the context of the proposed amendments and issues for comment.

A. Issues for Comment Related to Victims

1. Whether the term "victim" as used in USSG § 2B1.1 should include individuals whose privacy was violated, but who suffered no monetary harm, as a result of the offense (§ 209(b)(12))

The Commission has requested comment on whether the definition of "victim" should be expanded to include those whose privacy was violated but who did not suffer monetary harm. The Commission should not expand the definition of victim to include those who did not suffer monetary harm.

First, the Commission has already studied the extent to which the number of individuals whose privacy was violated is an appropriate measure of the seriousness of the offense in identity theft cases (where this issue is most likely to arise) and determined that reliance on the number of victims alone "can result in either overstating or understating the harm." *See* USSC, *Identity Theft Final Report*, at 26 (Dec. 15, 1999). It may overstate the harm in simple identity theft crimes where a means of identification is fraudulently used but was not used to "breed" additional forms of identification. It may understate the harm in a case where a means of identification is used to obtain other means of identification without the victim's knowledge. *Id.* The latter circumstance is more likely to cause non-monetary harms that are difficult to measure, such as harm to reputation or credit rating, and for that reason the Commission created a specific offense characteristic to apply where an offender uses one means of identification to "breed" another means of identification. *See* USSG § 2B1.1(b)(10)(C) & comment. (backg'd); *see also* USSG, App. C, Amend. 596 (Nov. 1, 2000).

Second, courts are invited to upwardly depart whenever the "guideline substantially understates the seriousness of the offense," including when the court perceives that the number of individuals whose personal data was stolen warrants a higher sentence. USSG § 2B1.1, comment. (n.19(A)). Upward departure is invited where the offense "caused or risked substantial non-monetary harm," such as "a substantial invasion of privacy," USSG § 2B1.1 comment. (n.19(A)(ii)), and when the defendant "essentially assumes" the identity of an individual by producing or obtaining numerous means of identification. USSG § 2B1.1 comment. (n.19(A)(vi)(III).[21]

[21] *See, e.g.*, *United States v. Shough*, 239 Fed.Appx. 745 (3d Cir. 2007) (affirming upward departure under Note 19(A)(vi) where defendant essentially assumed victim's identity and caused substantial harm to victim's credit rating).

Third, identity theft offenses by their nature involve the misuse of personal information. Many individuals, however, are not aware that their identifying information has been obtained or misused, and so do not subjectively experience an invasion of privacy. Only about one-quarter of those who know about the misuse of their identifying information report, as a primary concern, the emotional toll resulting from the invasion of privacy.[22] Absent data showing that courts are frequently imposing above-guideline sentences on the basis of privacy violations, the Commission should not broaden the definition of "victim."

We have seen no data indicating that sentences in these cases are not sufficient already. To the contrary, with the passage of the Identity Theft Penalty Enhancement Act in 2004, Congress created a two-year, minimum mandatory, consecutive sentence to be imposed where identity theft is committed in relation to a broad range of federal felony offenses. *See* 18 U.S.C. § 1028A(a)(1) and (b). This statute already provides more than adequate punishment for identity theft**.**

2. Whether persons who suffer no "loss" because any pecuniary harm was immediately reimbursed should nonetheless be treated as "victims" under USSG § 2B1.1(b)(2)

This is not a concern of Congress; it is not included in its directive. Rather, it was first introduced by the Department as a "circuit split" in need of resolution. However, there is no split. For those reasons and others, detailed below, the Commission should not act on this issue.

Currently, for an individual to be counted as a "victim" under § 2B1.1(b)(2), he or she must have suffered "actual loss," which is defined as "pecuniary harm," or "harm that is monetary or that otherwise is readily measurable in money." "Loss" does not include emotional distress, harm to reputation, or other non-economic harm. USSG § 2B1.1, comment. (n.1, 3(A)(i), (iii)). Thus, pecuniary harm that is immediately reimbursed by a third party is not treated as a "loss," and the individual reimbursed is not treated as a "victim."

The issue for comment suggests that courts may not agree about whether individuals whose temporary financial losses were entirely reimbursed by third parties may be counted as victims. However, this is not so. As recently explained by the Court of Appeals for the Third Circuit, courts do in fact agree that an individual should not be counted as a "victim" under § 2B1.1(b)(2) unless he suffered some harm that was not fully reimbursed which can be measured in terms of money. *United States v. Kennedy***,** __ F.3d __, 2009 U.S. App. LEXIS 2120, 2009 WL 250105 (3d Cir. Feb. 4, 2009) (collecting and harmonizing cases). In fact, all of the decisions cited in the issue for comment agree that an individual who is fully reimbursed for temporary financial losses

---

[22] FTC Report at 52-53 & fig. 21.

is not a victim under § 2B1.1(b)(2), but that there "may be situations in which a person could be considered a 'victim' under the Guidelines even though he or she is ultimately reimbursed." *Id.* at *10-11 (quoting *United States v. Yagar*, 404 F.3d 967, 971 (6th Cir. 2005)). This might occur if the person suffered some other "adverse effect" that can be readily measured in terms of money. *Id.* Contrary to the suggestion in the issue for comment, the court in *United States v. Lee*, 427 F.3d 881, 895 (11th Cir. 2005), did not hold that a person is a victim if he or she suffered a loss at the time of the offense regardless of any remedial action. Rather, the court held that certain creditors who had repossessed collateral could be counted as "victims" because they were not fully reimbursed for their monetary loss.

As the court in *Kennedy* ultimately concluded, in those unusual circumstances in which an offender's culpability may not be adequately covered by the current definition of "victim," the answer is not to insist upon "formalistic technicalities" and "mathematical calculation," but to recognize that a district court retains the discretion to account for that added culpability:

> We expect that district judges will examine the particular facts of each case in fashioning a just sentence without getting bogged down in formalistic technicalities. Sentencing is not a mathematical calculation; it is a human enterprise that requires wisdom, judgment, and old-fashioned common sense. To the extent that the plain language of the Guidelines – including its Commentary and Application Notes – would lead to unfair results, we repose our confidence in district judges to apply fairly and justly the factors set forth in 18 U.S.C. § 3553(a), which may require variances from the Guidelines ranges.

Kennedy, *supra*, at *18. The Commission should repose the same level confidence in the district courts, rather than create a rule that would overstate the seriousness of the offense in most cases, and introduce further difficulty into the guidelines.

The issue for comment does not say how the Commission might count persons who were immediately reimbursed and thus suffered no pecuniary harm as victims. The Department has suggested, however, that the Commission amend the definition of loss in Application Note 3 to include as "actual costs" any "lost time," including "lost time in restoring credit."[23] No such change should be made.

First, it is unnecessary, as Application Note 19(A)(ii) invites upward departure if "the offense caused or risked substantial non-monetary harm." Second, it would overstate the seriousness of the offense and add complexity and difficulty to the sentencing process for no good reason. Victims of crime typically do spend some time, energy or emotion dealing with the crime, which is generally why the conduct is a crime. The Commission adds points for pecuniary harm because it considers this an extra harm, on top of the ordinary time and effort, and because it is readily measurable. If the

[23] DOJ Letter at 8.

Commission were to adopt a new principle of counting harms that are ordinary and not measurable in money, this would be unfair because it would overstate the seriousness of the offense, and it would be too difficult for courts to administer within the confines of a sentencing hearing. How would judges evaluate matters like the reasonableness of the length of time spent, or the way in which the time was spent? Would "lost time" include time during which the person was emotionally distressed? Would a thin-skinned person count as a victim, but a thick-skinned person would not?

As shown by the survey conducted by the Federal Trade Commission, more than half of the individuals whose identifying information was misused incurred no out-of-pocket expenses.[24] Although all of them reported that they spent time resolving problems resulting from offenses, with a median of four hours,[25] thirty percent spent one hour or less.[26] Only ten percent reported spending at least 55 hours.[27] A rule that would count as "victims" those who suffered non-pecuniary harm runs the risk of counting every person whose information was obtained or accessed. This could be just a few, or it could be millions. Further, such a rule would result in arbitrary application, depending not on culpability or measurable harm, but very often on the manner in which a company deals with the breach. Some companies inform individuals that the security of their personal information has been compromised, and it is up to the individual to monitor credit reports, change account information, etc. Other companies say nothing and immediately correct any problem, so no individual spends any time dealing with it.

For all of the reasons above, we oppose changing the definition of "loss" or "victim" to account for non-monetary harm. If the Commission must act, it can create a special rule for identity theft convictions that adds a one-level enhancement if any person, otherwise not counted as a victim under § 2B1.1(b)(2), reasonably spent 50 hours or more resolving financial problems resulting from the offense. This would require that any added punishment be based on proof that the offense resulted in aggravated, non-pecuniary harm substantially beyond that which ordinarily occurs as the result of identity theft.[28] And this proof would be based on an objective reasonableness standard, which comports with the standard for restitution in identity theft cases under 18 U.S.C. § 3663(b)(6).

[24] FTC Report, at 6.

[25] *Id.* at 2, 39 & tbl. 2.

[26] *Id.* at 5-6 & tbl. 2.

[27] *Id.*

[28] *Id.* (10% reported spending over 55 hours).

B. The extent to which the offense violated the privacy rights of individuals (§ 209(b)(5))

The Commission has proposed two options for revising USSG § 2H3.1 to take account of this factor in wiretapping offenses under 18 U.S.C. § 2511. The Commission should not adopt either proposal.

Option One would add a specific offense characteristic that would add increasing levels depending on the number of individuals whose "personal information or means of identification" was "involved" in the offense. It would clarify that the means of identification must be of an identifiable (not fictitious) individual, and would define "personal information" as "sensitive or private information involving an identifiable individual" with several examples, such as medical records, e-mail, and photographs "of a sensitive or private nature."

The proposed specific offense characteristic would not accurately distinguish between more and less culpable defendants. Under the current guideline, the guideline range for a first offender who intercepted, without doing anything more, an email that "involved" the personal information of a number of individuals, would be 4-10 months, in Zone B of the Sentencing Table. However, under Option One, the same offender would have his offense level increased by up to six levels, to a range of 18 to 24 months in prison, more than quadrupling the sentence based on conduct that is not clearly tied to increased culpability or even likelihood of harm.

Guideline increases based on toting up the number of persons whose personal information was "involved" is not an appropriate proxy for offense seriousness or offender culpability, and will often overstate the seriousness of the offense. Most would agree that the offender described above, who intercepted a great deal of personal information but did nothing with it, is *less* culpable than the offender who intercepts, uses, or discloses the personal information of only one person and manages to cause considerable harm to that single person. For that individual, § 2H3.1 already invites an upward departure. *See* USSG § 5H3.1 comment. (n.5(ii)).

Without data indicating that guideline sentences for § 2511 offenses are not high enough, or that § 2511 offenses "involving" personal information actually present increased harm, the Commission should not adopt Option One.

Option Two would suggest an upward departure "if the offense involved . . . personal information [or] means of identification . . . of a substantial number of individuals." While preferable to Option One, adding another enumerated example to the upward departure provision at Application Note 5(i) would add complexity to an area already within the total discretion of the sentencing judge, in conflict with the Commission's goal of simplification. More important, it would expand upon the directive. Section 2H3.1 applies to many offenses other than those addressed by Congress in § 209(a) of the Act, ***i.e.***, 18 U.S.C. §§ 119, 1039, and 1905. The

Commission should refrain from expanding upward departures for offenses the Commission was not asked to consider.

The issue for comment asks if the extent to which the offense violated the privacy rights of individuals is adequately addressed by existing provisions in § 2B1.1. It is, and we oppose any additional enhancements. Section 2B1.1(b)(15)(A) provides a 2-level enhancement for offenses under 18 U.S.C. § 1030 that involved an intent to obtain personal information. In addition, for offenses not involving computer hacking, Application Note 19 provides for an upward departure for a variety of reasons, including if the offense "caused physical harm, psychological harm, or severe emotional trauma or resulted in a substantial invasion of privacy interest." These provisions are sufficient to account for violation of privacy interests beyond that ordinarily occurring in computer crimes or offenses involving the misuse of identifying information.

C. Whether the defendant disclosed personal information obtained during the commission of the offense (§ 209(b)(13))

For offenses involving convictions under 18 U.S.C. § 1030, the guidelines provide a two-level enhancement if the offense "involved an intent to obtain personal information." USSG § 2B1.1(b)(15)(A)(i)(II). Personal information is defined as:

> sensitive or private information (including such information in the possession of a third party), including (i) medical records, (ii) wills, (iii) diaries; (iv) private correspondence, including e-mail; (v) financial records; (vi) photographs of a sensitive or private nature; or (vii) similar information.

Id. § 2B1.1, comment. (n.13(A)). In 2003, the Commission reported that for offenses involving computer fraud under 18 U.S.C. § 1030 and sentenced under § 2B1.1, "approximately one-third involved an intent to obtain personal information."[29] In 2007, the enhancement was applied in only 21 cases, or 0.2% of cases sentenced under § 2B1.1.[30]

To the extent that disclosure may cause additional harm in § 1030 cases or special harm in identity theft cases, courts are encouraged to depart upward if the "offense caused physical harm, psychological harm, or severe emotional trauma, or resulted in a substantial invasion of privacy." USSG § 2B1.1 comment. (n.19(A)(ii)).

As such, § 2B1.1 provides courts with sufficient tools to account for disclosure of personal information. Absent data indicating that these provisions are inadequate to account for disclosure of personal information, the Commission should not act.

---

[29] Cyber Crimes Report at 11.

[30] 2007 Guideline Frequencies, at 12.

D. The potential and actual loss resulting from the offense: reduction in value of, or cost of developing proprietary information obtained from, a protected computer (§ 209(b)(3))

Congress directed the Commission to consider whether the guidelines adequately account for "the value of information obtained from a protected computer, regardless of whether the owner was deprived of use of the information," and "where the information obtained constitutes a trade secret or other proprietary information, the cost the victim incurred developing or compiling the information." *See* Pub. L. No. 110-326, § 209(b)(3). In response, the Commission has proposed two options to amend § 2B1.1 to address the meaning of "loss" with respect to offenses involving proprietary information. We oppose both.

First, there is no evidence that courts have been unable to calculate potential or actual loss as currently defined in § 2B1.1 in the circumstances described by the directive. Indeed, cases show the opposite. In *United States v. Ameri*, 412 F.3d 893 (8th Cir. 2005), the defendant was convicted, *inter alia*, of theft of trade secrets in the form of computer software for which there was not a verifiable "fair market value" and no "repair" of the software was involved. *Id.* at 895. The district court included the cost of development as a major component of its loss calculation, which the court of appeals affirmed. *Id.* at 900-01. In *United States v. Four Pillars Enter. Co.*, 253 Fed. Appx. 502 (6th Cir. 2007), the district court granted the government's request to consider the research and development cost of proprietary formulas obtained by the defendant, which the government then proved to be approximately $869,300. *Id.* at 512 (affirming loss calculation).

Second, Application Note 3(C) states that in estimating loss, a court can consider "[t]he reduction that resulted from the offense in the value of equity securities or ***other corporate assets***." (emphasis added). This language covers any reduction in the value of a corporation's proprietary information.

Third, for any remaining case that might involve harm not covered by the definition of loss in the guideline and Application Note 3, Application Note 19 invites upward departure if "the offense created a risk of substantial loss beyond the loss determined for purposes of subsection (b)(1)," or if "the offense caused or risked substantial non-monetary harm" USSG § 2B1.1, comment. (n.19(A)(ii), (iv)) (2008).

Contrary to the Department's suggestion, there is no need to "clarify" that courts can account for such loss. Doing so would not only add complexity to the guideline when simplification is a priority, but would create a categorical definition that could result in dramatic, and unwarranted, increases in some cases. For example, there could be cases in which the information was not destroyed or rendered useless, perhaps due only to the timing of the offense, the cost of research and development far exceeds the market value of the information. If anything, the Commission should clarify that relying on development costs as a measure of loss should be a last resort only, to be used when ordinary methods of measuring loss do not reasonably account for the harm caused. This

circumstance might occur in cases in which the proprietary information is completely destroyed or rendered useless.

Absent evidence that courts frequently impose above-guideline sentences to account for the kinds of loss identified in § 209(b)(3), the Commission should not add unnecessary complexity to an already complex guideline or make changes that would result in guideline ranges that significantly overstate culpability.

In addition, Option 2 would unjustifiably expand the directive because it would apply to all offenses sentenced under § 2B1.1, not just those offenses involving computers or identity theft that Congress addressed in the directive.

E. Level of sophistication and planning involved in such offenses (§ 209(b)(1))

The Commission addressed this factor with respect to § 1030 offenses in 2003, in response to the directive, set forth at section 225(b)(2) of the Homeland Security Act of 2002, Pub. L. No. 107-296, to ensure that the guidelines and policy statements applicable to offenses under 18 U.S.C. § 1030 adequately accounted for the level of sophistication involved in the offense. *See* USSG, App. C, Amend. No. 654 (Nov. 1, 2003). After reviewing data on 116 defendants sentenced for violations of § 1030, the Commission concluded that the special offense characteristic now at USSG § 2B1.1(b)(9)(C), which adds two levels (regardless of the offense) "if the offense . . . involved sophisticated means," adequately accounts for increased culpability when the offense involves "especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense." USSG § 2B1.1 comment. n.(8(B)); *Cyber Crimes Report* at 8. According to the data, "many 18 U.S.C. § 1030 offense are relatively unsophisticated."

The Department contends that this is no longer the case, citing the November 2008 testimony of a representative of the Business Software Alliance, stating that "cybercrime is increasingly technologically sophisticated," that "proxy" or "zombie" computers are increasingly used to conceal location, and that systems known as "botnets" are used to create vast, surreptitiously controlled computer networks to commit cybercrime.[31] That technology has advanced, however, does not necessarily mean that offenses have become more serious or deserve enhanced punishment.

1. "Sophisticated means" and § 2B1.1(b)(9)(C)

The Commission has now proposed to add to Application Note 8(B) of USSG § 2B1.1 the following broad example of sophisticated means: "In a scheme involving computers, using any technology or software to conceal the identity or geographic location of the perpetrator ordinarily indicates sophisticated means."

[31] DOJ Letter at 2.

First, the language of subsection (b)(9)(C), as defined in Application Note 8, already encompasses the use of technology or software that is "especially complex or especially intricate . . . pertaining to the execution or concealment of the offense." The Department has not suggested that courts have been unable to account for the use of such technology or have been forced to depart or vary at substantial rates due to the absence of a specific example. Adding another example runs counter to the Commission's goal of simplifying the guidelines. The Commission should leave it to courts to consider on a case-by-case basis whether the use of a particular form of technology or software truly constitutes sophisticated means.

Second, the proposed example will almost certainly sweep in offenders who do not merit an increase for sophisticated means. Our research indicates that the use of technology or software to conceal identity or location does ***not*** always involve especially complex or intricate conduct and does ***not*** always make the offense more difficult to detect. Many individuals and companies use proxy computers to route their Internet traffic as a matter of course and for reasons unconnected to criminal activity, such as protecting privacy, increasing efficiency, or controlling access. Easily accessible sources provide simple instructions for setting up a proxy computer,[32] and most web browsers allow a person to route Internet activity through a proxy with just a few clicks of a mouse. That the ***design*** of a particular computer program or computer function is technically sophisticated does not mean that an individual using it has ***himself*** done anything intricate or complex.[33]

Further, in addition to the sophisticated means enhancement under § 2B1.1(b)(9)(C), § 3B1.3 provides for a two-level upward adjustment in any case in which the defendant "used a special skill [] in a manner that significantly facilitated the commission or concealment of the offense." Although courts have held that a defendant's use of self-taught computer skills can warrant an increase under § 3B1.3, the skills at issue must be more than those possessed by the general public. [34] As explained by the Sixth Circuit in a case involving counterfeit currency:

---

[32] ***See, e.g.***, Floss Manuals, ***Bypassing Internet Censorship***, http://en.flossmanuals.net/CircumventionTools (an extensive "living" manual written collaboratively and in partnership with Sesawe, an Internet consortium working to support uncensored access to the Internet, covering topics such as Simple Tricks, Using a Web Proxy, Installing a Proxy, PHProxies, Switch Proxies, Using TOR, and providing resources for thousands of web proxies).

[33] ***See*** Graeme R. Newman, U.S. Dept. of Justice, Office of Community Oriented Policing Services, No. 25, ***Identity Theft***, at 11 (June 2004) ("[T]he ways offenders steal identities are decidedly low-tech. Computer hackers aren't necessarily geniuses; sometimes they simply obtain a password by trickery or from a dishonest insider."); Graeme R. Newman & Megan M. McNally, ***Identity Theft Literature Review***, at 4 (in a research support submitted to the Department of Justice, explaining that in scams to obtain personal information, "the majority of these types of fraud use relatively tried and true old scams adapted to new technologies").

[34] ***See*** USSC § 3B1.3, comment. (n.4); ***see also, e.g.***, ***United States v. Prochner***, 417 F.3d 54, 61 (1st Cir. 2005) (affirming application of § 3B1.3 where defendant used a "high and unusual level of [self-taught] computer know-how" to hack into secure website); ***United States v. Petersen***, 98 F.3d 502, 507 & n.5 (9th Cir. 1996) (holding that self-taught ability to hack into computer systems warrants special skill assessment under § 3B1.3, but cautioning that "computer skills cover a wide spectrum of ability. Only where a

> Computer skills on the order of those possessed by Godman, by contrast, can be duplicated by members of the general public with a minimum of difficulty. Most persons of average ability could purchase desktop publishing software from their local retailer, experiment with it for a short period of time, and follow the chain of simple steps that Godman used to churn out counterfeit currency. Godman's computer skills thus are not "particularly sophisticated" as suggested by the *Petersen* case.
>
> At a time when basic computer abilities are so pervasive throughout society, applying § 3B1.3 to an amateurish effort such as Godman's would threaten to enhance sentences for many crimes involving quite common and ordinary computer skills. The Guidelines contemplate a more discriminating approach.

United States v. Godman, 223 F.3d 320, 323 (6th Cir. 2000). By adding an enhancement to § 2B1.1 that covers "any technology or software," the Commission would create a categorical increase under § 2B1.1 that is inconsistent with several courts' interpretation of the special skills enhancement currently set forth in § 3B1.3 as applied in cases involving computer skills.

There may be unusual fraud offenders who do more than use readily available software or possess skills not ordinarily possessed by the general public, perhaps by writing their own especially complex software to conceal identity or by creating a complex surreptitious system to take over the computers of others without their consent and to do harm. For such an offender, § 2B1.1 already instructs courts to take the aggravated nature of the conduct into account, both through the loss table and through the current definition of "sophisticated means." Moreover, the guideline range can be further increased by two levels under § 3B1.3, even if the defendant's computer skills are self-taught.[35]

Third, as originally conceived, the enhancement for sophisticated means was expressly limited to conduct that is "significantly more complex or intricate than the conduct that may form the basis for an enhancement for more than minimal planning." *See* USSG, App. C, Amend. No 587 (Nov. 1, 1998) (amending former § 2F1.1). More than minimal planning, in turn, referred to "offense behavior involving affirmative acts on multiple occasions." USSG § 2B1.1, comment. (backg'd) (2003). The underlying rationale was that "planning and repeated acts are indicative of an intention and potential

---

defendant's computer skills are particularly sophisticated do they correspond to the Sentencing Commission's examples of "special skill"— lawyer, doctor, pilot, etc.").

[35] *See United States v. Minneman*, 143 F.3d 274, 283 (7th Cir. 1998) (affirming application of enhancements for both sophisticated means and special skill under based on the same conduct); *United States v. Olis*, 429 F.3d 540, 549 (5th Cir. 2005) (district court engaged in no impermissible double counting to apply both enhancements for sophisticated means and special skills where defendant "used his special skills in accounting and tax matters to advance an extremely sophisticated, but fraudulent, scheme").

to do considerable harm. Also, planning is often related to increased difficulties of detection and proof." *Id.* In 2003, when the Commission eliminated the enhancement for more than minimal planning for fraud and theft offenses, it did so for two reasons: "to obviate the need for judicial fact-finding about this frequently occurring enhancement and to avoid the potential overlap between the more than minimal planning enhancement and the sophisticated means enhancement." In other words, some amount of planning is intrinsic to theft and fraud offenses and is accounted for by the structure of the guideline. The sophisticated means enhancement should apply only when the offense involves *especially* complex or intricate conduct.

Finally, by adding a broad example to Application Note 8(B) covering any type of proxy computer, regardless of actual sophistication, the Commission would effectively relieve the government of proving that the defendant engaged in especially complex or intricate conduct aimed at concealing identity or location. Given the liberty interests at stake, the Commission should not create an enhancement for the use of any technology or software that conceals identity or geographic location – applicable to every case governed by § 2B1.1 involving a computer, not just § 1030 offenses – regardless of the actual sophistication involved.

2. Self-taught computer skills and § 3B1.3

The Commission asks whether § 3B1.3 should apply to a person who has self-trained computer skills. As set forth above, courts have had no difficulty applying § 3B1.3 to those whose skills are truly specialized rather than commonplace. There is no need to further complicate the guidelines by articulating that the provision applies to those with self-trained computer skills. If the Commission must include language that unequivocally includes a person who is self taught, it should make clear that the self-trained computer skills must be "particularly sophisticated" for the adjustment to apply. *See United States v. Godman*, 223 F.3d 320, 323 (6th Cir. 2000) (citing *United States v. Petersen*, 98 F.3d 502, 507 & n.5 (9th Cir. 1996)).

F. Whether such offense was committed for purpose of commercial advantage or private financial benefit (§ 209(b)(2))

In 2003, also in response to Congress's directive at section 225(b)(2) of the Homeland Security Act of 2002, Pub. L. No. 107-296, the Commission considered whether the guidelines adequately account for computer crimes committed for the purpose of commercial advantage or private financial benefit, and did not amend § 2B1.1 based on this factor because "commercial advantage and private financial benefit are typical motivations in offenses sentenced under § 2B1.1, . . . and the structure of the guideline takes this into account." *Cyber Crimes Report* at 8-9. This conclusion is still sound and there is no reason to believe otherwise.

The Department, however, urges the Commission to amend § 2H3.1, which applies to wiretapping offenses under 18 U.S.C. § 2511, to provide for increased punishment if the offense was committed for the purpose of commercial gain or private

financial benefit. We disagree. First, § 2H3.1 already recommends a three-level enhancement if the purpose of the offense was to obtain direct or indirect commercial advantage or economic gain, bringing the base offense level to 12. *See* USSG § 2H1.3(b)(1)(B). Depending on the defendant's criminal history, the guideline range is 10 to 37 months, *see* USSG ch. 5, pt. A (Sentencing Table). Second, under Application Note 5 of § 2H3.1, judges are invited to depart upward (to the statutory maximum of five years if necessary) if the offense level "substantially understates the seriousness of the offense."

According to the Commission's data for 2008, there were no above-guideline sentences for any reason in cases sentenced under § 2H3.1. Thus, there can be no empirical basis to conclude that § 2H3.1 does not adequately account for offenses committed for the purpose of commercial advantage or private financial benefit.

G. Whether the defendant acted with intent to cause either physical or property harm in committing the offense (§ 209(b)(4))

No action is necessary in response to this directive. In 2003, the Commission addressed the similar directive set forth at section 225(b)(2) of the Homeland Security Act of 2002, Pub. L. No. 107-296. At the time, the Commission increased punishment by approximately 50% for damage to a protected computer under 18 U.S.C. § 1030(a)(5)(A)(i) to account for increased penalties "and the heightened level of intent involved in such violations." *See Cyber Crimes Report* at 4, 9; USSG App. C, Amend. No. 654 (Nov. 1, 2003); USSG § 2B1.1(b)(15)(ii) (2008).

The guidelines fully account for a defendant's intent to cause physical or property damage in the following ways:

- Under § 2B1.1, punishment increases incrementally based on the amount of pecuniary damage caused.
- Section 2B1.1 provides for a two-level enhancement if the offense involved "the conscious or reckless risk of death or serious bodily injury." USSG § 2B1.1(b)(13) (2008).
- Section 2B1.1 contains a cross-reference when "the conduct set forth in the count of conviction establishes an offense specifically covered by another guideline in Chapter Two." *Id.* § 2B1.1(c)(3)(C) & comment. (n.15).
- The commentary to § 2B1.1 suggests an upward departure where the offense level substantially understates the seriousness of the offense "if the primary objective of the offense was an aggravating, non-monetary objective," or "[t]he offense caused or risked substantial non-monetary harm," including death resulting from a § 1030 offense. USSG § 2B1.1 comment. (n.19(A)(ii)).
- Upward departure is encouraged under § 5K2.2 (Physical Injury), "if significant injury resulted," and under § 5K2.5 (Property Damage or

Loss), "if the offense caused property damage or loss not taken into account within the guidelines."

H. Whether the offense involved a computer used by the United States Government, a State, or a local government in furtherance of national defense, national security, or the administration of justice (§ 209(b)(7))

Whether the defendant's intent to cause damage or intent to obtain personal information should be disaggregated and considered separately from other factors set forth in § 2B1.1(b)[(15)] (§ 209(b)(11))

In 2003, in response to Congress's directive, the Commission added a two-level enhancement under § 2B1.1 for offenses under 18 U.S.C. § 1030 if the offense involved (1) "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," or (2) "an intent to obtain personal information." USSG, App. C., Amend. No. 654 (Nov. 1, 2003); USSG § 2B1.1(b)(15)(A)(i)(I-II) (2008).

As structured, this enhancement, which corresponded to an approximate 25% increase in sentences, will be superseded by greater enhancements under the same subsection if the offense also involved intentionally damaging a protected computer under § 1030(a)(5)(A)(i) (a 50% increase) or if it caused substantial disruption of a critical infrastructure (roughly doubling the sentence). As the Commission explained to Congress, the graduated levels "ensure incremental punishment for increasingly serious conduct, and were chosen by the Commission in recognition of the fact that conduct supporting application of a more serious enhancement will frequently encompass behavior relevant to a lesser enhancement as well." *See Cyber Crimes Report* at 4.

At the time, Commission data indicated that approximately 33% of 116 cases under 18 U.S.C. § 1030 would have received a two-level enhancement based on the defendant's intent to obtain personal information, and approximately 5% would have received a two-level increase because the offense involved a computer system used to maintain a critical infrastructure. Another 14.4% would have received the four-level adjustment for intentional damage to a protected computer, and no cases would have received the six-level enhancement for disrupting a critical infrastructure. ***See id.*** It is not clear from the data how many offenses involved conduct covered by more than one enhancement.

In keeping with the Commission's stated rationale for structuring these enhancements as incrementally increased punishment for incrementally more serious offenses, the Commission should not disaggregate the factors in subsection (b)(15)(A)(i) from each other or from in subsection (b)(15)(A). Transforming these factors into cumulative enhancements for 18 U.S.C. § 1030 offenses runs the risk of cumulative punishment for conduct that often overlaps. Further, § 2B1.1 applies to a large number

statutory provisions beyond the five expressly addressed by the directive here. Separate enhancements based on these factors that might apply to all offenses covered by § 2B1.1 would unjustifiably expand the scope of the directive.

In addition, Application Note 19 invites upward departure where the guideline range understates the seriousness of the offense. For example, if aggregation under subsection (b)(15) results in a single upward enhancement that does not adequately account for the harm caused to privacy interests, the court can depart upward if the "offense caused or risked substantial non-monetary harm," such as a "substantial invasion of privacy interest." USSG § 2B1.1 comment. (n.19(A)(ii)) (2008). A court can also account for aggravated harms in the case of stolen information from a protected computer under 18 U.S.C. § 1030(e)(2) if the defendant sought the stolen information to further a broader criminal purpose. *Id.* § 2B1.1 comment. (n.19(A)(v)) (2008).

Absent data demonstrating that the Commission's rationale for aggregating the factors in subsection (b)(15) was flawed or results in sentences that generally do not reflect the seriousness of the offense, the Commission should not take any action in response to these directives.

I. Remaining factors and issues for comment

Absent empirical evidence that the guidelines are inadequate with respect to the remaining factors or any other issue for comment, the Commission should not act.

V. MITIGATING CIRCUMSTANCES

Congress also instructed the Commission to "account for any additional aggravating or mitigating circumstances that might justify exceptions to the generally applicable sentencing ranges." Pub. L. No. 110-326, § 209(c)(2). The Commission has requested comment regarding whether there are other aggravating or mitigating factors involving identity theft and computer offenses that might justify an amendment. As in our letter of December 8, 2008, we propose adding a non-exhaustive list of factors to Application Note 19, as follows:

> (C) Downward Departure Considerations.---There may be cases in which the offense level determined under this guideline substantially overstates the seriousness of the offense. In such cases, a downward departure may be warranted. The following is a non-exhaustive list of factors that the court may consider in determining whether a downward departure is warranted:
>
> (i) A primary objective of the offense was a non-aggravating, non-monetary objective. For example, a primary objective of the offense was to gain access to one's own work product or to assist another person in accomplishing a non-aggravating, non-monetary objective.

(ii) The offense was committed through the use of readily available computer technology, software, or hardware, which persons of average computer skills are able to operate.

(iii) The defendant acted promptly after law enforcement detection or apprehension to assist in ensuring that personal information obtained was not disseminated, or that personal information disclosed was not further disseminated.

(iv) The defendant successfully participated in a restorative justice meeting involving both the defendant and the victim. For purposes of this departure ground, "restorative justice meeting" means a face-to-face meeting moderated by a trained third party mediator in which the defendant and the victim reach agreement on reasonable steps the defendant will take to repair the harm done to the victim.

Although we believe each of these factors would help to balance the ever-upward structure of § 2B1.1, we believe the final factor warrants especially serious consideration. Restorative justice practices can mitigate the harm caused by fraud offenses by holding offenders accountable to victims in a manner unlike traditional forms of punishment and by offering non-monetary reparation.[36] They may also have a deterrent effect, both specific to the offender being sentenced and in general with respect to others in the community within which the offender lives and works.[37] Restorative justice practices can be used to justify mitigated sentences and to justify plea bargains.[38]

As suggested by one U.S. Attorney, who became a believer in restorative justice practices after studying them as a Fulbright fellow in New Zealand:

> If an agreement is reached and fulfilled, then, the prosecution and defendant could jointly report on the conference and the agreement to the sentencing court. The parties could also in some cases seek a downward departure . . . based on the defendant's successful participation in a restorative justice process. In other words, introducing restorative responses as part of the plea bargain process benefits the stakeholders affected by the crime, mitigates some of the problems associated with the

[36] Zvi D. Gabbay, *Exploring the Limits of the Restorative Justice Paradigm: Restorative Justice and White-Collar Crime*, 8 Cardozo J. Conflict Resol. 421, 466-71(2007).

[37] *Id.* at 450 (citing studies suggesting that shaming, embarrassment, and social censure may have a deterrent effect on white collar crime).

[38] *Id.* at 449-50, 471.

extensive use of plea bargains and is procedurally feasible under current law.[39]

Currently, § 2B1.1 measures the relationship of the defendant to a victim or victims only by increasing punishment. Restorative justice practices, in contrast, give voice to victims, to offenders, and to community representatives, often revealing "deeper understandings of what has led to criminal acts and what is needed to reintegrate the offender into the community and to restore the victim, restorative justice conferences and other processes frequently lead to the greater use of and need for community resources (including drug/alcohol counseling, alternative education programs, and community service opportunities)."[40]

The Commission should take this opportunity to exercise its recent commitment to exploring alternative means of serving the purposes of sentencing by including in § 2B1.1 an express recognition that restorative justice can help to repair harm, prevent future crimes of the defendant and possibly others, and restore the community. Adopting the language proposed here will encourage parties to utilize restorative justice meetings, and in the process, address Congress's concern with deterrence while furthering other purposes of sentencing.

[39] *Id.* at 471-72 (internal quotation marks omitted) (citing Donald D. Schmid, Ian Axford Fellowship Report, *Restorative Justice in New Zealand: A Model for U.S. Criminal Justice*, 54-56 (Aug. 2001), available at www.fulbright.org.nz/voices/axford/docs/schmidd.pdf)).

[40] *New Zealand is at the cutting edge of restorative justice, according to American prosecutor Donald Schmid*, Te Ara Whakatika (newsletter of the court-referred Restorative Justice Project in New Zealand), August 2001, Issue # 3, available at http://www.courts.govt.nz/pubs/newsletter/tearawhakatika/issue-3.html.

FEDERAL DEFENDER OFFICE
DISTRICT OF MASSACHUSETTS
408 ATLANTIC AVENUE, 3RD FLOOR
BOSTON, MASSACHUSETTS 02110

TELEPHONE: 617-223-8061
FAX: 617-223-8080

December 8, 2008

Hon. Ricardo H. Hinojosa, Chair
United States Sentencing Commission
One Columbus Circle, N.E.
Washington, DC 20002-8002

Re: Public comment on Commission action in response to Pub. L. 110-326, § 209 (a directive relating to identity theft and computer crimes).

Dear Judge Hinojosa:

I want to thank you and your staff again for asking me to speak on behalf of the Federal Defenders at the Commission's briefing on November 20, 2008. I did not submit a written statement on that date, but would like to do so now with the comments set forth below. The directive in § 209 of Pub. L. 110-326 asks the Commission to study thirteen factors in the context of five statutes. These comments are not meant to address each factor in all its possible permutations. I do, however, seek to share with you some of our initial responses to the directive, in the hope that they will be useful to you at this stage of the amendment cycle. We look forward to working with the Commission and submitting further comment as the amendment process unfolds.

At the outset, I should note that we are struck by the fact that the Commission has already studied and responded to the substance of many of the factors enumerated in § 209, particularly with respect to offenses proscribed by 18 U.S.C. § 1030. Absent evidence that the guidelines in their present form do not adequately address concerns raised in the directive, we see little need for further action. Moreover, to the extent that any amendments to the guidelines would raise sentences in identity theft cases, we note that with the passage of the Identity Theft Penalty Enhancement Act in 2004, Congress provided for a two-year, minimum mandatory consecutive sentence to be imposed where identity theft is committed in relation to a broad range of federal felony offenses. *See* 18 U.S.C. § 1028A(a)(1) and (b). It is the position of the Federal Defenders that this statute punishes severely enough, and in many instances too severely, the crime of identity theft and the concomitant invasion of privacy which that offense entails.

We offer the following additional observations, which I have arranged to correspond generally to the factors as they appear and are numbered in the directive.

§ 209(b)(1) The level of sophistication and planning involved in such offense.

The Commission addressed this factor with respect to 18 U.S.C. § 1030 offenses in 2003. In section 225(b)(2) of the Homeland Security Act of 2002, Pub. L. 107-296, Congress directed the Commission to ensure that the guidelines and policy statements applicable to § 1030 offenses adequately account for the level of sophistication involved in the offense. *See* USSG, App. C, Amend. No. 654 (Nov. 1, 2003). After reviewing data on 116 cases, the Commission concluded that the special offense characteristic now at USSG § 2B1.1(b)(9)(C), which adds two levels "if the offense . . . involved sophisticated means," adequately accounts for increased culpability when the offense involves "especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense." USSG § 2B1.1 comment. (n.8(B)); *see* USSC, *Report to Congress: Increased Penalties for Cyber Security Offenses*, at 8 (May 2003) [*Cyber Crimes Report*]. At the time, the Commission's data "suggest[ed] that many 18 U.S.C. § 1030 offense are relatively unsophisticated."

At the hearing held on November 20th, the representative of the Department of Justice suggested that the Commission should now amend Application Note 8(B) to specify that the use of computer proxies constitutes "sophisticated means." As described by the Department, offenders are increasingly using proxies to commit computer crimes, making it harder to detect the offense and apprehend the offender.

We believe that the Commission should not add another enumerated example to Application Note 8(B). First, the term "sophisticated means" as defined in the first sentence of Application Note 8(B) is broad enough to encompass situations in which the use of a proxy constitutes sophisticated means.[1] The Department has not suggested that courts have been unable to account for the use of proxies, or have been forced to depart at substantial rates, because of the absence of an enumerated example. Without some evidence that the guidelines do not adequately account for the use of proxies, the Commission should not act.

Second, it is not at all clear that the use of proxies always involves especially complex or intricate conduct, or that it always makes the offense more difficult to detect. As technology advances, what once was sophisticated becomes commonplace. We would hazard to guess that a significant number of people today consider the use of a proxy to be a relatively basic technological function that is neither intricate nor complex. The Commission should avoid creating what would amount to a presumptive enhancement for the use of a proxy – applicable to every case governed by § 2B1.1 – unless the government can demonstrate that the technique used in a given case necessarily involved the special complexity and intricacy for which the enhancement was intended.

[1] The first sentence of Application Note 8(B) provides that "'sophisticated means' means especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense."

Third, adding proxies as an enumerated example runs counter to the Commission's goal of simplifying the guidelines. By the time the Commission has amended Application Note 8 to add proxies as an example, technology may well have advanced to yet another form of sophisticated concealment in computer crimes, rendering proxies obsolete and requiring yet another example to keep pace. Indeed, any example of "especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense" is subject to rapid obsolescence. Instead of continually adding or amending examples in response to cutting-edge technology, the Commission should leave it to the sentencing court to determine whether the use of the particular technology in the case before it constitutes sophisticated means.

§ 209(b)(2) Whether such offense was committed for purpose of commercial advantage or private financial benefit.

The Commission also addressed this factor with respect to 18 U.S.C. § 1030 offenses in 2003. At the time, the Commission did not amend the guidelines to increase sentences under § 2B1.1 based on this factor because "commercial advantage and private financial benefit are typical motivations in offenses sentenced under § 2B1.1, . . . and the structure of the guideline takes this into account." *Cyber Crimes Report* at 8-9. There is no indication that this conclusion is no longer sound with respect to offenses sentenced under § 2B1.1.

With respect to 18 U.S.C. § 2511 wiretapping offenses sentenced under § 2H3.1, we do not believe that the Commission should amend that guideline to provide for increased punishment if the offense was committed for the purpose of commercial gain or private financial benefit. First, § 2H3.1 already provides for a three-level enhancement if the purpose of the offense was to obtain direct or indirect commercial advantage or economic gain, bringing the base offense level to 12. *See* USSG § 2H1.3(b)(1)(B). Depending on a defendant's criminal history, the resulting sentence recommended by the guidelines is a term of imprisonment ranging from 10 to 37 months, *see* USSG ch. 5, pt. A (Sentencing Table).

Second, increasing the offense level to further account for commercial gain would reduce the utility of the upward departure provisions at Application Note 5 of § 2H3.1. Under the current structure of § 2H3.1, courts can account for commercial gain and still find room to depart upward as necessary in those cases in which the offense level does not adequately account for the seriousness of the invasion of privacy or value of protected information. If the offense level is automatically increased in all cases resulting in commercial gain, courts will have less room to account for the gradations in harms addressed by Application Note 5.

The Commission should only consider amending the guidelines if its review of data indicates a significant rate of upward departure in wiretap cases on the basis that § 2H3.1 does not adequately account for commercial or private gain. If the Commission does amend the guideline, it should take the opportunity to eliminate the flat three-level increase for any amount of commercial gain in order to ensure that a defendant whose financial gain is minimal is no longer considered the same as a

defendant whose financial gain is substantial. *See, e.g.*, § 2B5.3 (Criminal Infringement of Copyright or Trademark) (adding no levels if the infringement amount is $2,000 or less, and only one level if the infringement amount exceeds $2,000 but is less than $5,000).

§ 209(b)(3) The potential and actual loss resulting from the offense[.]

Congress has directed the Commission to consider whether the guidelines adequately account for "the value of information obtained from a protected computer, regardless of whether the owner was deprived of use of the information," and in the case of trade secrets or other proprietary information, "the cost the victim incurred developing or compiling the information." *See* Pub. L. No. 110-326, § 209(b)(3).

We have not found any evidence that courts are finding it difficult to calculate potential or actual loss as currently defined in § 2B1.1 in the circumstances described by the directive. Indeed, it appears that courts readily consider the development costs of proprietary information in calculating loss. In *United States v. Ameri*, 412 F.3d 893 (8th Cir. 2005), the defendant was convicted, *inter alia*, of theft of trade secrets in the form of computer software for which there was no verifiable "fair market value" and no "repair" of the software was involved. *Id.* at 895. The court held that the district court did not err in its calculation of loss, which included as a major component the cost of development. *Id.* at 900-01. And in *United States v. Four Pillars Enter. Co.*, 253 Fed. Appx. 502 (6th Cir. 2007), the district court granted the government's request to consider the research and development cost of proprietary formulas obtained by the defendant, which the government then proved to be approximately $869,300. *Id.* at 512 (affirming the calculation of loss).

In addition, Application Note 3(C) states that in estimating loss, a court can consider "[t]he reduction that resulted from the offense in the value of equity securities or *other corporate assets*." (emphasis added.) This language should adequately cover dilution in the value of a corporation's proprietary information.

For any remaining case that might involve loss not specifically addressed in the guideline and Application Note 3, courts may consult Application Note 19, which allows for upward departure if "the offense caused or risked substantial non-monetary harm" or if "the offense created a risk of substantial loss beyond the loss determined for purposes of subsection (b)(1)." USSG § 2B1.1 comment. (n.19(A)(ii), (iv)) (2008).

Contrary to the suggestion by the Department, the result in *United States v. Levine*, 477 F.3d 596 (8th Cir. 2001), does not suggest that the guidelines need to be amended to account for the cost to the victim of developing proprietary information. The government in *Levine* did not ask the district court to consider the development costs incurred by Acxiom Corporation, the victim in the case, in calculating loss under § 2B1.1. Rather, the government requested the court to calculate loss based on the government expert's estimate of the fair market value of the information illegally obtained (an estimate of over $58 million). *See United States v. Levine*, No. 4:04CR00175 (E.D.

Ark.), Gov't Sentencing Mem. at 6-10. The defendant challenged that calculation, arguing that, based on the opinion of his own expert witnesses, the fair market value of the information obtained was less than $5,000. *See id.*, Def.'s Sentencing Mem. at 18. In the alternative, the defendant argued that the maximum reasonable loss calculation could be based on the value of the information as stipulated in a related case, also based on the fair market value, which placed the loss at $893,000. *See Levine*, 477 F.3d at 603. The court ultimately calculated the loss at $850,000, presumably based on the competing suggestions of fair market value. Although the court did depart upward, it did not do so to account for development costs or dilution in the value of the information. *See United States v. Levine*, No. 4:04CR00175 (E.D. Ark.), Sent. Tr. at 348-49.

In short, we believe that, absent evidence that courts are too often forced to rely on upward departures in order to account for the kinds of loss addressed by this directive, the Commission should not add unnecessary complexity to a guideline that is already quite complex.

§ 209(b)(4) Whether the defendant acted with intent to cause either physical or property harm in committing the offense.

The Commission also addressed this factor with respect to 18 U.S.C. § 1030 offenses in 2003. At the time, the Commission increased punishment by approximately 50% for damage to a protected computer under 18 U.S.C. § 1030(a)(5)(A)(i) to account for increased penalties "and the heightened level of intent involved in such violations." *See Cyber Crimes Report*, at 4, 9; USSG App. C, Amend. No. 654 (Nov. 1, 2003); USSG § 2B1.1(b)(15)(ii) (2008).

In addition to incrementally increasing punishment on the basis of the pecuniary damage caused, § 2B1.1 provides for a two-level enhancement if the offense involved "the conscious or reckless risk of death or serious bodily injury," USSG § 2B1.1(b)(13) (2008), and the commentary suggests an upward departure where the offense level substantially understates the seriousness of the offense "if the primary objective of the offense was an aggravating, non-monetary objective," or "[t]he offense caused or risked substantial non-monetary harm." *See* USSG § 2B1.1, comment. (n.19(A)(i) and (ii)). Death resulting from a § 1030 offense was specifically enumerated in 2003 as a basis for upward departure. *See* USSG § 2B1.1, comment. (n.19(A)(ii)).

Finally, § 2B1.1 contains a cross-reference if "the conduct set forth in the count of conviction establishes an offense specifically covered by another guideline in Chapter Two." *Id.* § 2B1.1 (c)(3)(C).

With the foregoing provisions, courts have sufficient guidance to account for a defendant's intent to cause physical or property damage.

§ 209(b)(5) The extent to which the offense violated the privacy rights of individuals.

§ 209(b)(8) Whether the offense involved a computer used by the United States Government, a State, or a local government in furtherance of national defense, national security, or the administration of justice.

§ 209(b)(11) Whether the defendant's intent to cause damage or intent to cause personal information should be disaggregated and considered separately from other factors set forth in § 2B1.1(b)[(15)].

In 2003, in response to Congress's directive, the Commission added a two-level enhancement in § 2B1.1 for 18 U.S.C. § 1030 offenses where the offense involved (1) "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," or (2) "an intent to obtain personal information." USSG, App. C., Amend. No. 654 (Nov. 1, 2003); USSG § 2B1.1(b)(15)(A)(i)(I-II) (2008).

As structured, this enhancement (which corresponded to an approximate 25% increase in sentences) will be superseded by greater enhancements under the same subsection if the offense also involved intentionally damaging a protected computer under 18 U.S.C. § 1030(a)(5)(A)(i) (resulting in a 50% increase in sentence) or if it caused substantial disruption of a critical infrastructure (roughly doubling the sentence). As the Commission explained to Congress, the graduated levels "ensure incremental punishment for increasingly serious conduct, and were chosen by the Commission in recognition of the fact that conduct supporting application of a more serious enhancement will frequently encompass behavior relevant to a lesser enhancement as well." *See Cyber Crimes Report*, at 4.

At the time, the Commission indicated that approximately 33% of the cases it studied would have received a two-level enhancement based on the defendant's intent to obtain personal information. Another very small number of defendants would have received a two-level increase because the offense involved a computer system used to maintain a critical infrastructure. Another 14.4% would have received the four-level adjustment for intentional damage to a protected computer. No case would have received the six-level enhancement for disrupting a critical infrastructure. *See id.*[2]

In keeping with the Commission's rationale for structuring these enhancements in a manner which provides for incremental punishment, we do not believe that the Commission should disaggregate the factors in subsection (b)(15)(A)(i) from each other or from the other factors. First, changing these factors to cumulative enhancements for 18 U.S.C. § 1030 offenses would risk

[2] It is not clear from the data how many offenses involved conduct covered by more than one enhancement, if any.

excessive punishment. Second, separate enhancements based on these factors that might apply to all offenses covered by § 2B1.1 would stray beyond the discrete statutory provisions addressed by Congress's directive here.

In addition, Application Note 19 already allows courts to increase sentences as necessary in those cases in which the guideline range understates the seriousness of the offense. For example, if aggregation under subsection (b)(15) results in a single upward enhancement that does not adequately account for the harm caused to privacy interests, the court can depart upward if the "offense caused or risked substantial non-monetary harm," such as a "substantial invasion of privacy interest." USSG § 2B1.1 comment. (n.19(A)(ii)) (2008). The court could also account for aggravated harms in the case of stolen information from a protected computer under 18 U.S.C. § 1030(e)(2) if the defendant sought the stolen information to further a broader criminal purpose. *Id.* § 2B1.1 comment. (n.19(A)(v)) (2008).

Absent data or feedback from the courts demonstrating that the Commission's rationale for aggregating the factors in subsection (b)(15) was flawed, or results in sentences that generally do not reflect the seriousness of the offense, the Commission should not take any action in response to these directives.

§ 209(b)(12) Whether the term "victim"as used in USSG § 2B1.1, should include individuals whose privacy was violated as a result of the offense in addition to individuals who suffered monetary harm as a result of the offense.

Directive 12 of Pub. L. 110-326 asks the Commission to consider whether the definition of "victim" in USSG § 2B1.1 should be expanded to include anyone whose privacy was violated as a result of the offense, in addition to individuals who suffered monetary harm. We oppose such an expansion on several grounds.

First, this issue is most likely to arise in the context of offenses involving identity theft, and the directive essentially asks the Commission to consider the extent to which the number of victims is an appropriate measure of the seriousness of the offense. The Commission has already studied this question,[3] however, and determined that reliance on the number of victims alone "can result in either overstating or understating the harm." *See* USSC, *Identity Theft Final Report*, at 26 (Dec. 15, 1999). The number of victims may overstate the harm in simple identity theft crimes where a means of identification is fraudulently used but not bred; it may understate the harm in a case where a means of identification is used to obtain other means of identification without the victim's knowledge. *Id.* The latter circumstance is more likely to cause significant emotional distress to the victim, and for that reason the Commission created a specific offense characteristic to apply in cases involving bred means of identification. *See* USSG § 2B1.1(b)(10)(C) & comment. (backg'd).

[3] *See* Pub. L. No. 105-318, Oct. 30 1998, at § 4(b)(1).

Second, the "non-monetary" harm perhaps most frequently cited by victims of affirmative identity theft is the loss of time associated with attempts to repair one's credit. Though typically thought of as a non-pecuniary harm, lost time can in fact be monetized and, when it is, the loss amount may be added to the loss figure determined under USSG § 2B1.1(b)(1), and the victim counted as a "victim" for guideline purposes under USSG § 2B1.1(b)(2). *See United States v. Armstead*, ___ F.3d ___, 2008 WESTLAW 4570608 (9th. Cir. Oct. 15, 2008); *United States v. Abiodun*, 536 F.3d 162, 167-69 (2d Cir. 2008). Importantly, in this regard the guidelines define "victim" co-extensively with those who may obtain restitution under 18 U.S.C. § 3663, which was amended by Pub. L. No. 110-326 to permit restitution in identity theft prosecutions for "the value of the time reasonably spent by the victim in an attempt to remediate the intended or actual harm[.]"

Third, where a court perceives that the number of individuals whose personal data was stolen in a given case is extraordinary, and not otherwise accounted for in determining the base offense level, the court may upwardly depart pursuant to USSG § 2B1.1, comment. (n.19).[4] That is precisely what the district court did in *United States v. Uyaniker*, 184 Fed. Appx. 856 (11th Cir. 2006).[5] Absent data which shows that courts are routinely upwardly departing on this basis, the Commission should not broaden the definition of "victim" beyond its current parameters.

Finally, if the Commission broadens the definition of "victim" in USSG § 2B1.1, sentences for some defendants in identity theft cases will be raised. We have seen no data which indicates that sentences in these cases are not sufficient already. To the contrary, with the passage of the Identity Theft Penalty Enhancement Act in 2004, Congress provided for a two-year, minimum mandatory, consecutive sentence to be imposed where identity theft is committed in relation to a broad range of federal felony offenses. *See* 18 U.S.C. § 1028A(a)(1) and (b). As stated above, we believe that this statute provides more than adequate punishment for the crime of identity theft.[6]

---

[4] Application Note 19(A)(vi) enumerates upward departure grounds where a victim (or victims) suffered extraordinary non-pecuniary harm, and that provision appears to provide sufficient guidance in such cases. *See, e.g., United States v. Shough*, 239 Fed.Appx. 745 (3d Cir. 2007)(affirming upward departure where defendant essentially assumed victim's identity and caused substantial harm to victim's credit rating).

[5] Although the opinion in *Uyaniker* is less than clear on this point, the Eleventh Circuit affirmed a district court's four-level upward departure based on the fact that the defendant had stolen and used the identities of 78 people. A transcript of the sentencing hearing is on file with the undersigned.

[6] *See* Erik Camayd Freixas, *Interpreting after the Largest ICE Raid in US History: A Personal Account*, June 13, 2008, *referenced in* Editorial, *The Shame of Postville, Iowa*, N.Y.Times, July 13, 2008, available at http://www.nytimes.com/2008/07/13/opinion/13sun 2.html?scp=3&sq=postville&st=cse. A copy of Dr. Camayd Freixas 'article is attached.

§ 209(c)(2) [M]itigating circumstances that might justify exceptions to the generally applicable sentencing ranges[.]

At the meeting on November 20th, Commissioner Howell asked whether the Defenders could articulate mitigating factors which might constitute grounds for downward departures in identity theft or computer crimes cases. We appreciate the invitation to speak to this issue, and are considering proposals to submit in this regard. We begin by offering the following proposed language to be added to Application Note 19:

(C) Downward Departure Considerations.---There may be cases in which the offense level determined under this guideline substantially overstates the seriousness of the offense. In such cases, a downward departure may be warranted. The following is a non-exhaustive list of factors that the court may consider in determining whether a downward departure is warranted:

(i) A primary objective of the offense was a non-aggravating, non-monetary objective. For example, a primary objective of the offense was to gain access to one's own work product or to assist another person in accomplishing a non-aggravating, non-monetary objective

(ii) The offense was committed through the use of readily available computer technology, software, or hardware, which persons of average computer skills are able to operate.

(iii) The defendant acted promptly after law enforcement detection or apprehension to assist in ensuring that personal information obtained was not disseminated, or that personal information disclosed was not further disseminated.

(iv) The defendant successfully participated in a restorative justice meeting involving both the defendant and the victim. For purposes of this departure ground, "restorative justice meeting" means a face-to-face meeting moderated by a trained third party mediator in which the defendant and the victim reach agreement on reasonable steps the defendant will take to repair the harm done to the victim.

Finally, we understand that the Commission will be analyzing data as part of the study prompted by Pub. L. 110-326, § 209. We hope that you will share the results of that data analysis with us.

Sincerely,

/s/ J. Martin Richey
J. Martin Richey,
Assistant Federal Public Defender

Jennifer Coffin, Staff Attorney
Sentencing Resource Counsel

On Behalf of the Federal Public and Community Defenders and the Federal Defender Sentencing Guidelines Committee

cc: Hon. Ruben Castillo, Vice Chair
Hon. William K. Sessions III, Vice Chair
Commissioner Michael E. Horowitz
Commissioner Beryl A. Howell
Commissioner Dabney Friedrich
Commissioner Ex Officio Edward F. Reilly, Jr.
Commissioner Ex Officio Jonathan Wroblewski
Judith M. Sheon, Staff Director
Ken Cohen, General Counsel
Kathleen Grille, Deputy General Counsel