

420 7th St., NW
Apt. 510
Washington, DC 20004

January 24, 2003

United States Sentencing Commission
One Columbus Circle, N.E.
Suite 2-500
Washington, D.C. 20002-8002
Attention: Public Affairs

Dear Judge Diana E. Murphy:

Thank you for allowing me to comment on two of the amendments to the Sentencing Guidelines that you and the rest of the Commission are currently considering.

Use of Body Armor in a Crime of Violence or Drug Trafficking Crime:

First, the adjustment increase should be limited only to defendants who use body armor during commission of the crime. Obviously, when Congress directed increased punishment for anyone committing a violent crime "in which the defendant used body armor," it imagined a defendant clad in body armor while shooting at police officers. By using a broader definition, the Sentencing Commission may encompass more use of body armor than Congress imagined. In this instance, the Commission should be conservative in issuing its mandate. Accordingly, the amendment to the Sentencing Guidelines should only encompass crimes in which the defendant wore body armor during commission of the crime.

More importantly, Congress has mandated an increase of at least two levels to the adjustment. The Commission should not expand beyond the mandated two level increase for any reason. The higher the increase, the longer the defendant will be in jail, which deprives the defendant of his freedom for a greater amount of time, while consuming additional taxpayer money. And for what use? The difference between two, four, or six levels will have no deterrent effect on crime: criminals will not base their use of body armor on the potential penalty if they get caught. Clearly, if they are in such a war-mentality to be wearing body armor, the defendants do not believe they will ever find themselves in court. Nor will such a penalty reform a criminal in such a manner to additionally condition him not to use body armor when committing crime in the future. This increase will simple be a tool for more legal wrangling for prosecutors and defense lawyers, and an avenue for allowing vengeance into our courtrooms. Please, do not increase the sentencing for body armor use any more than is absolutely mandated by Congress.

The 21st Century Department of Justice Appropriations Authorization Act: Sentencing Level Increases

This is a general comment to your numerous questions spurn from this Act concerning whether you should increase the punishment associated with certain level adjustments. As stated above concerning increases for body armor, I do not believe that increasing penalties will help deter crime: criminals do not consider the minutia of adjustments before they commit crimes, as they

usually do not know of the adjustments and do not believe or care if they get caught. Additionally, given the types of crimes considered in the Act, it seems unlikely that additional years in prison will help reform such criminals. Furthermore, increased incarceration time means increase cost to taxpayers; we should keep imprisonment costs down by limiting sentencing as much as possible. Indeed, the increased adjustments will serve only one purpose: to allow victims of the crime, through the court, to exact additional revenge on the criminals. Revenge is the worst of human characteristics and should not be embodied in the laws of our great nation! The courts should not be given tools with which to channel the vengeance of victims or the community on criminal perpetrators, no matter how heinous their crimes. By keeping the adjustments and sentences in general as low as possible, we ensure that the courts of this country dispense justice, not vengeance.

Thank you for allowing me to comment on these issues.

Faithfully yours,



Lee F. Berger

SEAN P. DEVEREUX, P.A.

ATTORNEY AT LAW
The Jackson Building
22 South Pack Square, Suite 1100
Asheville, North Carolina 28801

TEL: (828) 285-9455
FAX: (828) 285-9457

BOARD CERTIFIED SPECIALIST IN CRIMINAL LAW

E-MAIL ADDRESS: sdevereux@devereuxlaw.com

January 28, 2003

U.S. Sentencing Commission
Attention: Public Affairs
One Columbus Circle, N.E.
Suite 2-500
Washington, DC 20002-8002

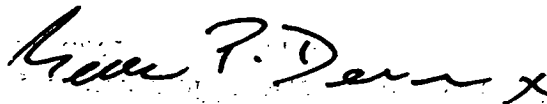
RE: Proposed amendment to §5G1.3

Dear Sirs,

I strongly urge the Commission to give retroactive application to the proposed amendment to U.S.S.G. §5G1.3. Defendants who were denied an adjustment of the length of their sentence due to the prior unsound distinction between discharged and undischarged terms of imprisonment should be given an opportunity to obtain appropriate relief *nunc pro tunc*.

I represent Charles McHan, Sr. who was the appellant in *United States v. McHan*, 101 F.3d 1027, 1040 (4th Cir. 1996)(holding that downward departure to allow an adjustment for a discharged term was based on an error of law and therefore was an abuse of discretion), cert. denied, 520 U.S. 1281 (1997). The Commission specifically disapproved the *McHan* decision in Amendment 645, effective No. 1, 2002. The prior amendment did McHan no good because it was not made retroactive. I hope the Commission will take this opportunity to make it possible for defendants such as McHan, who has suffered a grave injustice, to obtain relief.

Sincerely yours,



Sean P. Devereux

/tmh

REED WICKER PLLC

1120 Waterfront Plaza
325 West Main Street
Louisville, Kentucky 40202
(502) 572-2500 (phone)
(502) 572-2503 (fax)

Steven S. Reed
(502) 572-2501
steve@reedwicker.com

Kent Wicker
(502) 572-2502
kent@reedwicker.com

January 27, 2003

Honorable Diana E. Murphy
Chair
United States Sentencing Commission
One Columbus Circle, N.E., Suite 2-500
Washington, D.C. 20002-8002

In re: U.S. Sentencing Guidelines Amendments/Sarbanes-Oxley Act of 2002

Dear Judge Murphy:

This letter is in response to an invitation from the United States Sentencing Commission for public response to proposed revisions to the United States Sentencing Guidelines relevant to the Sarbanes-Oxley Act of 2002 ("Sarbanes-Oxley" or the "Act"). Much has been written on corporate criminal liability leading up to and since Sarbanes-Oxley and even more has been said. The purpose of this letter is not to join in the chorus of critics on either aisle of the debate. Rather, we draw upon our years of white collar crime prosecution and corporate criminal defense experience and offer insight regarding application of the Guidelines to organizations which have corporate compliance plans.

Our law firm focuses much of its practice on corporate investigations defense. Previously, Mr. Wicker and I served as the First Assistant U.S. Attorney and United States Attorney for the Western District of Kentucky, respectively, and we have more than 13 years of combined white collar crime prosecution experience as Assistant United States Attorneys. We have written on the subject of corporate criminal liability under Sarbanes-Oxley and Mr. Wicker teaches courses on Corporate Criminal Liability and Trial Practice at the Brandeis School of Law at the University of Louisville.

The preamble to Sarbanes-Oxley gives its purpose as "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities law, and for other purposes." The Act expands the prosecutor's arsenal by increasing criminal fraud penalties that companies and their employees face if convicted.

January 27, 2003

Page 2

The Act directs the Sentencing Commission to consider changing the Guidelines to "ensure that the sentencing guidelines and policy statements reflect the serious nature of securities, pension, and accounting fraud and the need for aggressive and appropriate law enforcement action to prevent such offenses." In short, the revised Guidelines must increase the penalty when corporate fraud is committed and must provide incentives to deter fraud from occurring. In non-legal terms, this may be appropriately referred to as the "stick" and the "carrot."

To enhance the penalty, or "stick," the Sentencing Commission has issued proposed emergency guidelines which increase the guideline penalties for fraud offenses which (1) are committed by an officer or director of a public company, (2) endanger the financial soundness of a public company, (3) effect large numbers of victims, (4) create a loss to victims of over \$100 million, or (5) involve more sophisticated obstruction of justice. We hope these measures are effective in punishing and deterring white collar crime.

The goals of the Act would be met, we believe, if the Sentencing Commission also enhances the "carrot." The Guidelines should be revised to enhance the reward to companies which have effective compliance plans. Although no corporate actions can guarantee against employee misconduct, effective compliance plans can help corporations prevent and detect employee misconduct before the misconduct implicates the justice system.

Creating and implementing compliance plans are time consuming and expensive. Thus, companies may be reluctant to undertake them, despite the broad benefit to the company and the public. The Sentencing Commission should take note and enhance the incentive for companies to have compliance plans. We have two suggestions. First, we encourage the Sentencing Commission to adopt a five-level reduction in the "culpability score," under U.S.S.G. § 8C2.5(f). A five-level reduction would equate to a fifty percent reduction in the fine range. Currently, the Court may grant a three-level reduction in the corporation's culpability score, which would decrease the fine range up to thirty percent. While a thirty percent reduction is indeed better than nothing, in all likelihood, the reduction would not cover the costs of creating and maintaining an effective compliance plan in the majority of cases. Thus, from a financial perspective, there is now insufficient incentive for companies to adopt compliance plans. Increasing the reduction under § 8C2.5(f) gives companies a financial incentive to prevent and deter crime.

Second, the Guidelines should provide for a downward departure at sentencing when the costs of implementing the compliance plan greatly exceed the company's gain from the wrongful conduct. Of course, any decision to grant a downward departure would remain with the judge after careful consideration of the company's good faith effort to have an effective compliance plan. A similar downward departure provision

January 27, 2003

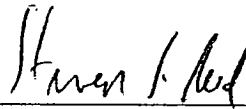
Page 3

already exists in § 8C4.9 in circumstances when the organization agrees to pay remedial costs which greatly exceed the organization's gain from the offense.

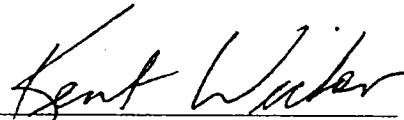
In sum, Congress has responded appropriately to the public's outcry over corporate scandals by increasing the statutory penalty for corporate fraud. If the Sentencing Commission follows Congress and gives prosecutors a bigger stick to fight corporate fraud, it should give corporations a juicier carrot to be responsible. That carrot is a sentence reduction when effective compliance plans have been implemented and a downward departure under proscribed circumstances.

We greatly appreciate your consideration. Please contact us if you have any questions.

Sincerely,



Steven S. Reed



Kent Wicker

REED WICKER PLLC

United States Sentencing Commission
Federal Judiciary Building
One Columbus Circle, N.E.
Washington D.C.
20002-8002

Attn: Office of Publishing and Public Affairs January 2, 2003

Dear Office of Publishing and Affairs:

I had previously sent a letter suggesting an improvement to the guidelines in the category of 'threatening communications' due to the vagueness and confusion caused by the large number of guidelines referenced under U.S.C. 876 in Appendix A of the guidelines manual.

I would ask that a retroactive amendment be made to the guidelines manual to be submitted in May of 2003 which changes the following sections of Appendix A.

Here is how it currently reads:



18 U.S.C. 875(a)	2A4.2, 2B3.2
18 U.S.C. 875(b)	2B3.2
18 U.S.C. 875(c)	2A6.1
18 U.S.C. 875(d)	2B3.2, 2B3.3
18 U.S.C. 876	2A4.2, 2A6.1, 2B3.2, 2B3.3
18 U.S.C. 877	2A4.2, 2A6.1, 2B3.2, 2B3.3

It appears from the way this part of Appendix A was written that it was intended for 18 U.S.C. 876 and 18 U.S.C. 877 to use guidelines in the same types of situations as 18 U.S.C. 875 has been sectioned off.

This is not what occurs in real practice. Because the guidelines have been listed 'together' under 18 U.S.C. 876 and 18 U.S.C. 877 prosecutors are simply using their 'discretion' as to which guideline to use.

In its current form, say a person is charged with 'Threatening to damage the reputation of another' under 18 U.S.C. 876 paragraph #4. Because all 4 guidelines are listed under 18 U.S.C. 876, a prosecutor can effectively use the highest - 2A4.2 (Demanding a ransom) for a 23 point base even though the title may be 'categorically incorrect' for this situation. This statute 876 paragraph #4 carries a maximum of 2 years in prison. 23 points is far above this range and a maximum sentence of 24 months ends up being placed against this individual.

I do not believe that this is how the commission originally wanted Statute 876 and 877 to be calculated and used.

I propose that the following amendments be made to this guideline and Appendix A in order to correct this situation:

#1.

That appendix A be amended as follows with changes shown in BOLD.

18 U.S.C. 875 (a)	2A4.2, 2B3.2
18 U.S.C. 875 (b)	2B3.2
18 U.S.C. 875 (c)	2A6.1
18 U.S.C. 875 (d)	2B3.2, 2B3.3
18 U.S.C. 876 (P. #1)	2A4.2, 2B3.2
18 U.S.C. 876 (P. #2)	2B3.2
18 U.S.C. 876 (P. #3)	2A6.1
18 U.S.C. 876 (P. #4)	2B3.2, 2B3.3
18 U.S.C. 877 (P. #1)	2A4.2, 2B3.2
18 U.S.C. 877 (P. #2)	2B3.2
18 U.S.C. 877 (P. #3)	2A6.1
18 U.S.C. 877 (P. #4)	2B3.2, 2B3.3

} THE Indictment should
define which paragraph
the defendant is being
Charged under.

#2.

That the statement in guideline 2A4.2 Demanding or Receiving Ransom Money in Application Note #1. "This section additionally includes extortionate demands through the use of the United States Postal Service, behavior proscribed by 18 U.S.C. 867-877."

be further clarified.

- Does it include ALL types of extortionate demands made by postal mail? (Is every extortionate demand a possible 23 point base?)

- Does it include only certain types of extortionate demands?

#3.

That the title of 2A4.2 be rephrased. 'Demanding or Receiving ransom money **IN A KIDNAPPING OFFENSE**'

(The background statement 'The actual demand for ransom under these circumstances is reflected in 2A4.1' is another statement which maybe could use some clarification.)

Such changes as listed above should counteract the use of 'Prosecutorial Discretion' is choosing a guideline in threat cases.

If these changes were made retroactive they would affect avery small group of the total Federal prison population.

Other modifications to this set of guidelines that I suggest:

#1. There are several "mathematical" point adjustments to 2B3.1 and 2B3.2 which would make more sense than the current version:

One difference that I noticed was that 2B3.2 has a "planning" enhancement of 3 points whereas 2B3.1 does not. This is really not reflected in the base level difference. If you commit a robbery, you have obviously "planned" it whereas that is not true of extortion necessarily.

As it reads now, if one committed a non violent robbery with planning they would have this many points:

Base 20 + no enhancement for planning. = 20 points

If one commits "extortion" with planning they receive:

Base 18 + 3 = 21 points

Technically, there is little difference in these two situations. Why should extortion be one point higher? If anything it should be equal or lower than robbery.

Two ways exist to remedy this:

- A. Change "planning" under 2B3.2 (b)(3)(B) to 2 levels enhance.
- B. OR change the base level for Robbery to 21.

#2. The application notes under "2B3.2" could be more clearly defined:

- Note #7 (Numerous victims) - define this further and its enhancement value.

- Note #8 (Threat to a family member) - define this further and maybe assign it a 1 point enhancement if the person "robbed, extorted or threatened" is a minor.

Also, additional commentary to Application note #2 of 2B3.2 could be added explicitly explaining that this guideline also applies to 'Threatening to kidnap', which I believe is not clear. The title of the 2B3.2 guideline could also be changed to 'Extortion by Force or Threat of Injury, Serious Damage or Kidnapping.'

#3, I also suggest the following changes to 5K2.13: Diminished Capacity.

I do not believe that the statement in 5K2.13 'the facts and circumstances of the defendant's offense indicates a need to protect the public because the offense involved a serious threat of violence' covers all cases. There are certain disorders such as Thyroid disease, Diabetes, etcetera which affect the blood chemistry and therefore also the mind temporarily. These two disorders among others are known to cause delusional or the occasional 'drunken' behavior in some cases (see the text 'Thyroid Solution' by Dr. Ridha Arem - 1999) which may render a defendant 'temporarily threatening'. Even if

a person makes a "statement of violence" who has a disorder that does NOT mean that such a person would ever act on it.

"Intoxication" is a VOLUNTARY reduction in mental capacity. INVOLUNTARY" reductions in mental capacity by way of disease have NOT been addressed in this downward departure or in the "culpability" standards of U.S.C. 875, 876 and 877.

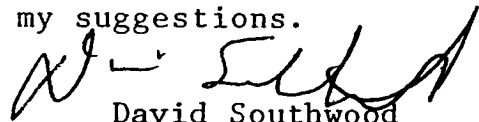
As an example, this year in my hometown we had a diabetic man who passed out while driving due to a low blood sugar level (they tested him right after). He swerved off the highway, hit several automobiles and then went off the road. Does this person really have a level of 'culpability' of recklessness or higher? Should such individuals be punished as criminals when they may present a TEMPORARY threat of violence?

I believe that maybe a downward departure should be allowed in cases of VERBAL or RECKLESS or NEGLIGENTLY committed acts of violence under 5K2.13 (2) instead of the current statement which allows no downward departures for the commission of any form of violent crime. In the cases of such downward departures the pre sentence report should both show that the defendant:

- A. Took responsibility for his actions
- B. Has "a disorder" which can affect the mind or emotions for short durations.
- C. That the person committed no physically violent act or verbally violent act with any malicious intent.
- D. That the person is not a drug user and that drugs were not involved with the threat or violent act.
- E. That the person agrees to further psychological counseling while in prison or on supervised release.

In my educated opinion, I believe that the above changes will solve the obvious flaws with this set of guidelines and add to uniformity and clarity in sentencing.

Thank you for your time in reading my suggestions.



David Southwood
#06534-028
Unit 9
FMCFP
PO Box 4000
Springfield, MO
65801-4000

Dear U.S. Sentencing Commission,

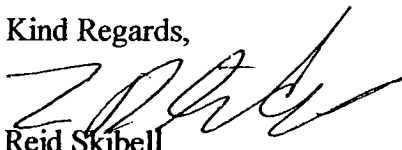
It would be a serious mistake to upgrade the penalties existing under 1030. I will summarize the general case against harsher penalties, and have attached a paper which more fully elaborates on my opposition to the proposed changes.

1. There is no evidence for a deterrent effect. This was the conclusion of the 1996 U.S. Sentencing Report, as it noted, "The limited empirical data available to the Commission and other factors preclude a definitive assessment of the deterrent effect of existing guidelines for computer fraud and computer vandalism." Little to no evidence has surfaced within the last seven years to support a conclusion that deterrence works in this context. Similarly, Indira Carr and Katherine Williams have found that high computer crime penalties in Singapore, Malaysia, and the UK have had little to no impact on the level of criminal activity. The decision calculus of the type of personalities that are attracted to computer crime offenses is simply not influenced by high penalty levels. Furthermore, even if there is a deterrent effect the current penalty levels are sufficiently severe to serve this purpose.
2. The Patriot Act changes mean that many low-level offenders are subject to the felony provisions of 1030. While minor trespassers should be subject to some punishment, upgrading the penalties under 1030 will do an injustice. The Patriot Act resulted in:
 - Expansion of 1030 (a)(2) – Asportation was originally reserved for military and financial documents, but now viewing any document which has an inherent value of more than \$5,000 is a felony offense.
 - Removal of the Computer Use Exception – Simply using computer time is now sufficient to classify as fraud under the CFAA
 - Aggregation of Damage – Financial harm can now be aggregated across many different computers to meet the monetary threshold for a felony.
 - Codification of the Definition of "Damage" from *US v. Middleton* – the *Middleton* court went beyond previous interpretations of 1030 to include the cost of damage assessments and forensic computer analysis, as well as intangible lost revenue from an interruption in service. The result is that any minor trespass can be held to have caused more than \$5,000 in damage.
3. Computer Crime is an Institutional Problem - Most computer crime is perpetrated by unsophisticated users who download scripts from the Internet. The only way that they are able to penetrate systems is that software producers knowingly ship software that has not been properly tested and is full of bugs, and network administrators are negligent in installing security patches. The culpability of these types of computer criminals is rather limited, and they should not be subject to harsh punitive sanctions simply as a scapegoat for those who do not take security seriously.

4. Computer Crime is not economically "cheaper" – Some have argued for harsher computer crime sanctions because computers make it far easier for a criminal to perpetrate a large scale crime. If anything, the opposite is true. Using a computer to commit a crime other than vandalism generally takes the sunk costs of many years of training. In those cases which it does not, this is only because of the negligence of others as explained in my third point.

For these reasons, and to avoid the injustice that will result from tougher criminal sanctions under 1030, I strongly urge the Sentencing Commission to refrain from upgrading the penalty structure under the Guidelines.

Kind Regards,



Reid Skibell

Columbia Law School
401 W. 118th st., B1
New York, NY 10027
reids@pobox.com

JANUARY 30, 2003

U.S. SENTENCING COMMISSION
ONE COLUMBUS CIRCLE N.E.
SUITE 2-500, SOUTH LOBBY
WASHINGTON, DC 20002-8002

PUBLIC COMMENT:
CONCURRENT SENTENCES

COULD THE SENTENCING COMMISSION TAKE IN CONSIDERATION, AND HELP THE FELONS THAT MOST NEED A CONCURRENT SENTENCE. THE FELONS THAT GET PUNISHED DOUBLE FOR THE SAME STATE CHARGE! THE FELONS THAT GET THERE FEDERAL CHARGE ENHANCED UNDER 4B1.2 BECAUSE OF THERE STATE CHARGE, THEN RUN CONSECUTIVE TO THE SAME STATECHARGE! THIS 4B1.2 SHOULD BE ONE OF THE MECHANISMS THAT TRIGGER A CONCURRENT SENTENCE. THE 4B1.2 IS COUNTED IN THE BASE OFFENSE LEVEL IN CHAPTER 4. THEY ARE THE MOST NEEDING THE CONCURRENT SENTENCE AND WOULD STOP THE DOUBLE COUNTING ON THEM FOR THE SAME STATE CHARGE. IT IS INCORPORATED IN THE BASE OFFENSE UNDER 4B1.2. SO THEREFORE IT SHOULD BE ADDED IN BESIDE RELEVANT CONDUCT 1B1.3 UNDER 5G1.3(B).

I ALSO READ RUGGIANO V. REISH 307 F3D 121. I AGREE WITH THAT COURTS SHOULD HAVE AUTHORITY UNDER 5G1.3(C) IN CASES THAT UNDER 4B1.2. KEEP THE DEFENDANT FROM BEING PUNISHED DOUBLE.

THANK YOU,

Stacy Burnett

RE: Public Comment (Pub L.107-296)

To whom it may concern:

I wish to comment on Section 225 of the Homeland Security Act of 2002.

With regards to cyber security, I would like to see Federal cyber laws that address the following issues:

DDoS and DoS – The malicious denial of Internet services by anyone should be treated as a terrorist act. This includes treating underage “script kiddies” who are responsible for a DDoS or DoS as criminals. The following link illustrates this thinking:
<http://grc.com/dos/grcdos.htm> .

Young children who deny Internet services to any company by attacking a private network cannot and should not do so without impunity. Sanctions against these children should be harsh. I would recommend 2 years in a Juvenile Detention Center and being banned from the Internet until age 18 for the “script kiddie” mentioned in the above Internet link.

The adults who are responsible for aiding and abetting these young children should face the stiffest possible sanctions. Ten years in prison would be a good start.

Virus and Trojan creators – Anyone who creates a virus or Trojan and then plants it on the Internet should be considered to be a criminal. Depending on intellectual property damage, that person should spend a minimum of 5 years in jail and be forbidden to use a computer for at least 5 years. Kevin Mitnick got off too easy in my opinion.

Cyber B/E – Breaking into a private network should be treated the same way as breaking into a private home.

Theft of data – Stealing the intellectual property of a private firm or individual is the same as breaking into a person’s home and stealing their goods.

Protecting Root Servers – Without the “root servers” there would not be an Internet. Crashing these servers through vandalism or some malicious act, should be treated the same as destroying a power grid to a major metropolitan area.

Therefore, root servers should be protected at all costs; with the highest level of security possible. This includes locating these servers in guarded buildings with internal and external alarm systems in place. A detailed background check should be done on all personnel in these secure locations.

Failure to adequately protect these servers – as determined by an outside auditor - should be treated as a felony.

Thanks for allowing me to comment:

Sincerely:

Dan Drass
Network Administrator

Dann Anthony Maurno
563 Sagamore Ave #12
Portsmouth NH 03801
603.436.3347
dmaurno@lillysoftware.com

United States Sentencing Commission
One Columbus Circle, N.E.
Suite 2-500
Washington, D.C. 20002-8002
Attention: Public Affairs

Re: Proposed Amendments to Sentencing Guidelines, Policy Statements and Commentary -
BAC2210-40/2211-01 (Dec 2002) (on "Cyberhacking")

Dear Sir/Madam:

I understand that this commission is seeking comments on sentencing for hacking and other cyber crimes, and respectfully submit the following.

It seems that, hacking being a non-violent crime, sentences are light, and sympathy low. But I can testify that it can be a psychologically devastating crime.

An individual against whom I obtained a restraining order used the internet to -

1. write to the sales and "request for information" addresses at my workplace
2. find phone/address/e-mail of my family and friends, and pester them with a barrage of messages
3. send threatening notes to me in the names of other people
4. send hostile notes to friends of her own, using my name, to rally support.
5. send blanket e-mails to friends and acquaintances with character assassinations.

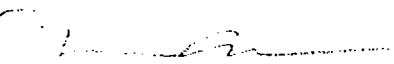
It was humiliating, to be on a business trip, only to receive a call from my company regarding the messages; to have to explain to my mother why she was receiving hostile e-mails entitled "Your Son's Behavior", and have to refute the lies therein; to have to explain to my former fiancée why she was receiving mail at her workplace from a perfect stranger wanting to "meet you to talk about how to love Dann," etc. I live in a small town (she moved here to be near me), and this poison is out there. I refuse to leave, but have no idea, day to day, who thinks what about me, because of this character assassination. The 'net was her weapon.

The individual pleaded "no contest" to five counts of violating a restraining order (bargained down from 10), plus two year's probation, a one-year extension of the restraining order (for a total of two years), and nine months court-enforced counseling. That was a stiffer sentence than the prosecutor had expected. But the judge refused to limit her access to the internet as unenforceable, and she continued to harass me through third parties.

Please, please recognize the intent of cybercrimes like these: to harm an individual as much as possible, and through clever and difficult-to-trace methods. The criminals use it with abandon, because they are shielded from the results. These crimes are too easy, and far more devastating than a click of a button would make them seem.

Thanks kindly for listening, and please do consider my letter.

Kind regards,


Dann Anthony Maurno

From: "Pat Castle 933" <p.castle@attbi.com>
To: <pubaffairs@ussc.gov>
Date: 1/14/03 12:58AM
Subject: Comments - on section 1030 of title 18, United States Code

The issue I'm commenting on:

BAC2210-40/2211-01

6. Cybersecurity

Issue for Comment: Section 225 of the Homeland Security Act of 2002 (the Cyber Security Enhancement Act of 2002), Pub. L. 107-296, directs the Commission to review and amend, if appropriate, the sentencing guidelines and policy statements applicable to persons convicted of an offense under section 1030 of title 18, United States Code, to ensure that the sentencing guidelines and policy statements reflect the serious nature of such offenses, the growing incidence of such offenses, and the need for an effective deterrent and appropriate punishment to prevent such offenses.

My comments:

It seems to me that crime (or vandalism) should not pay.

This suggests to me that the total penalties applied to the criminals should meet or exceed the total losses of the victims.

As an example: 1000 people each have to take an hour of their time to repair the damage done by one cyber attack. That's a loss of 1000 waking hours.

If only one in ten cyber attacks results in a conviction, then the penalty should be at least 10x the damages. In this example.... 10,000 waking hours. (Without this multiplier, the "odds are" that cyber attackers will have a gain of 9x, "losing" only 1/10 the time that was lost by the victims)

Since something like this is deliberate, the penalty should probably be tripled. I.e. 30,000 waking hours.

Of course, some of these attacks may cause physical or financial harm to victims, in which case penalties would have to take that into consideration.

Patrick M Castle

p.castle@attbi.com

816 S Heather Street

P.O. Box 166

Cornelius, OR 97113

[119]