COMPUTER CRIMES
&
COMPUTER / INTERNET BASED CHILD PORNOGRAPHY CRIMES

By:
G. Patrick Black
Federal Public Defender
Eastern District of Texas
110 N. College, Suite 1122
Tyler, Texas 75702
(903) 531-9233

Kenneth R. Hawk, II
Assistant Federal Public Defender
Eastern District of Texas
110 N. College, Suite 1122
Tyler, Texas 75702
(903) 531-9233

"If television's a babysitter, the Internet is a drunk librarian who won't shut up.."
– Patricia Briggs, Blood Bound

2014 Annual
National Seminar for Federal Defenders

Cleveland, Ohio
May 28-30, 2014

Table of Contents

I. INTRODUCTION 1

II. THE DEFENSE FOCUS: ON THE COMPUTER. 2

III. UNAUTHORIZED COMPUTER ACCESS (INTRUDERS/HACKERS), 18 U.S.C. § 1030. 3

A. 18 U.S.C. § 1030. 3
B. Sentencing Guidelines for § 1030. 5
C. Remote Access Tools "RAT". 6
D. "Blackshades". 6
E. Hackers Defense: the Trojan Horse. 6
F. Spyware Programs.. 7

IV. ILLEGAL CAPTURE, TRAFFICKING, AND POSSESSION OF COMPUTER ACCESS DEVICES AND PASSWORDS 18 U.S.C. § 1029 & 18 U.S.C. § 1030. 8

Current Trends in Access Device Fraud. 9

V. IDENTITY THEFT, 18 U.S.C. § 1028. 9

VI. CYBERSTALKING. 12

A. What Is Cyberstalking?. 12
B. Federal Cyberstalking Laws. 12

VII. INTERNET FRAUD 13

A. Introduction. 13
B. Online Drug Sales, Health Care, And Health Product Fraud. 14
C. Internet Auction Fraud. 15
D. Unlawful Internet Gambling Enforcement Act of "2006". 15
E. Internet Investment Scams. 17
F. New Anti Spam Legislation. 18

VIII. INTELLECTUAL PROPERTY CRIMES.. 19

IX. THE PRIVACY PROTECTION ACT OF 1980, 42 U.S.C. § 2000AA. 21

X. PORNOGRAPHY & THE INTERNET 22

A. Law Enforcement Operations

1. Historical Perspective. 22
2. Noteworthy Operations. 23
3. First Conviction Under Section 2251A of the Protect Act Since the Enhanced Penalties Became Effective. 24
4. Internet Providers to create database to combat child porn. 24

B. Computer Bulletin Boards, Definitions and Graphics Technology

1. Computer Bulletin Boards and Electronic Mail. 25
2. Child Pornography Definition. 25
   "Virtual Child Pornography". 26
   "Pseudo Child Pornography". 26

C. The Relevant Statutes

1. Protection of Children From Sexual Predators Act of 1998. 26
2. The Previous Version: 18 U.S.C. § 2252A. 27
3. The Earlier Version: 18 U.S.C. § 2252. 27
4 The 2003 PROTECT Act. 27
5. Child Protection Act of 2012. 28
6. Other Related Statutes. 28
7. Definitions, Elements, Jury Instructions, and Duplicative Charging. 28
   Visual Depictions. 28
   Mens Rea and Knowledge. 29
   Matters and Materials. 29
   Interstate Commerce. 30
   Production. 32
   Lasciviousness. 32
   Transmissions. 33
   Miscellaneous. 33
      1. Crime of Violence. 33
      2. Extraterritorial Application. 33
      3. Evidence Stipulation. 33
   Jury Instructions. 34
   Duplicative Charging. 34

D. Constitutional Issues and Case Law

1. Constitutional Challenges. 34
2. Communications Decency Act (the "CDA") and Child Online Protection Act (COPA). 35
3. Child Pornography Prevention Act of 1996 (the "CPPA"). 36
   A. Historical Perspective. 36
   B. Ashcroft v. Free Speech Coalition. 37

E. Pretrial Detention 37

Pretrial Release-Distribution / Transportation:
Electronic Monitoring Required. 38

F. Pretrial Hearings, Discovery, and Government Discovery Violations 39

G. Search and Seizure 41

H. Evidence: Medical Experts (Tanner Staging); Age of Child; Real Child 44

I. Entrapment, Impossibility, and Other Defenses

1. Affirmative Defenses. 46
   - Number of Depictions. 46
   - Subject was an Adult. 47
   - Good Faith Effort to Destroy or Report. 47
2. Entrapment. 47
3. Impossibility Defense. 48
4. The "Knowingly" Requirement of § 2252. 49
5. Sufficiency of the Evidence. 49

J. Sentencing Guidelines 49
1. A Judge's Struggle. 49
2. The "Feeney Amendment" and Departures. 50
3. 5K2.0 Departures. 51
4. §5K2.22. Specific Offender Characteristics as Grounds for Downward Departure in child Crimes and Sexual Offenses. 51
5. Booker/Fanfan Decided: A New Era in Federal Sentencing 52
6. Recent Sentencing Trends: Stabenow, Grober, Dorvee et al. 52
7 U.S.S.G. § 2G2.2. 54
8. Computer Enhancement. 55
9. Prepubescent Minor or Minor Children Under Age 12. 56
10. Distribution Enhancement. 56
11 Sadistic or Masochistic Portrayal Enhancement. 56
12. Pattern of Sexual Exploitation. 57
13. Minor Role Adjustment. 58
14. Use of Minor to Commit Crime. 58
15 Grouping. 58
16. Ten or More - Distinction Now Eliminated. 58
17. Diminished Capacity Departure. 59
18. Post-Offense Rehabilitation. 59
19. Susceptibility to Abuse. 59
20. Possession v. Distribution - Is there a Guideline difference?. 59

K. Restitution 60

L. Conditions of Supervised Release 61

M. Sex Offender Registration 62
1. Federal Law. 62
2. Texas State Law. 63
3. All 50 States Linked to Sex Offender Registry 63

X. Educating Yourself and the Judge 63

XI. Acknowledgment and Sources 64

APPENDIX 1 -- Online Resources

I. INTRODUCTION

"From Internet shopping to the electronic filing of taxes and the daily running of government and industry, the United States, like the rest of the world, is dependent upon computer networks that easily could be crippled by acts of cybercrime" according to Howard A. Schmidt, vice chair of the President's Critical Infrastructure Protection Board. The board was formed October 16, 2001, when then President Bush signed an executive order on critical infrastructure protection.

On September 18, 2002, the board released a report entitled "National Strategy to Secure Cyberspace." Then, to illustrate both the ongoing nature of the issue as well as its perpetual importance, on March 2, 2010, President Obama released his "Comprehensive National Cybersecurity Initiative" outlining his 12 part plan to secure and effectively control security in cyberspace. The plan builds on his predecessor's plan and recognizes the importance of the internet and its stability across Countries.
http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

Many federal agencies had made progress in the effort to secure the government's electronic systems from cyberthreats through public key infrastructure (PKI) and other initiatives, but as far back as a decade ago, the General Accounting Office (GAO) was reporting in its January 2014 Report that there was much work that remained to be done to finish the job. The 2004 report found that 20 of 24 government entities studied collectively spent $1 billion on PKI initiatives since 2001, a significant advance since the GAO first reported on the issue that year. Nonetheless, the GAO found that few agencies have been able to fully implement PKI. . The GAO report (GAO-04-157) is available at http://www.gao.gov/new.items/d04157.pdf

This persistent inability or unwillingness to meet the challenge to cybersecurity was again illustrated by the March 2009 testimony of David Powner, Director of Information and Technology Issues, who told one Subcommittee under the Committee of Homeland Security - the House Committee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, that the threat is persistent and the protections inadequate as he laid out 30 recommendations to strengthen the defense against cyber threats. This testimony is fascinating and can be found at http://www.gao.gov/new.items/d09432t.pdf.

Further, the United States' critical infrastructure is a "prime target" for cyber-terrorists, and threat of computer crime and its associated costs are soaring, according to an annual computer crime survey released in July 2003.

The majority of respondents to the "2006 Computer Crime and Security Survey" said they had detected computer security breaches within the last 12 months and had experienced financial losses due to computer breaches, the survey found.

Conducted by the Computer Security Institute (CSI) with the participation of the Federal Bureau of Investigation San Francisco Division's Computer Intrusion Squad, the 2006 survey tallied responses from 616 computer security practitioners at U.S. corporations, government agencies, medical institutions, and universities.

A survey released September 24, 2006, by the Pew Internet and American Life Project reflects that 58% of respondents believe that there will be a back lash against the internet and its pervasive presence in our lives that will manifest in the form of a self-segregating class of those who refuse to participate in on line resources who will also engage in acts of terrorism in protest.

The 2006 CSI survey is available at www.gocsi.com. The 2003 Pew survey is available at www.pewinternet.org.

The CSI survey indicated that the FBI, "in response to an expanding number of instances in which criminals have targeted major components of information and economic infrastructure systems," has established the National Infrastructure Protection Center (NIPC) located at FBI headquarters and the Regional Computer Intrusion Squads throughout the country.

In a partnership with federal agencies and private industry, the NIPC "is designated to serve as the government's lead mechanism for preventing and responding to cyber attacks on the nations' infrastructures," the survey stated.

The primary purpose of the FBI's Regional Computer Intrusion Squads (also called CHIP units) is to investigate violations of the Computer Fraud and Abuse Act. FBI computer teams will also focus on copyright and trademark violations, theft of trade secrets and economic espionage, theft of computer and high tech components, fraud, and other Internet crime, Ashcroft said.

The teams will also help train local, state and federal law enforcement in combating

computer crime.

Thirteen Regional FBI teams - in San Diego, Los Angeles, Seattle, Boston, Atlanta, Manhattan, Brooklyn, N.Y., Dallas, Portland, Sacramento and Alexandria, Va. have joined San Francisco, which pioneered the program. The locations were selected because of the high concentration of high-tech industry or growth in that industry, the presence of specialized FBI units, and "a significant number of cases already existing in those areas and other likely targets for computer intrusions or intellectual property crimes," according to former U.S. Attorney General John Ashcroft.

In addition to the 13 FBI Regional computer teams, there are 60 specialized computer teams that are focused on specific computer crimes.

In 2005, new CHIP units or Regional Computer Teams were created in the District of Columbia, Pittsburgh, Nashville, and Orlando.

The Billion Dollar "Big Challenge"

As far back as April 7, 2009, MSNBC reported in an online article that whether from bored teenagers, sophisticated nation-states or petty criminals, the Pentagon says it's under assault from computer hackers. Military leaders said that the Pentagon had spent more than $100 million for the six month period between October 2008 and April 2009 responding to and repairing damage from cyber attacks and other computer network problems.

Air Force Gen. Kevin Chilton heads the U.S. Strategic Command, which is responsible for protecting and monitoring the military's information grid. He says the motivations for the attacks include everything from vandalism to espionage. But whatever the source, Chilton says the attacks represent Strategic Command's "big challenge." [http://www.msnbc.msn.com/id/30090749/]

A SecurityWeek article from 2012 quoted industry analysts as projecting that the Federal Government will spend upwards of $13.5 billion annually by 2015 in efforts to secure Government computers and networks from intrusion and damage caused by unauthorized access. However, by the middle of 2013, the Pentagon alone was seeking $23 billion over the next 5 years to defend their data from Cyberattacks.

However, as the connection between Government and private industry information systems grows stronger, it's becoming increasingly clear that Government action alone may not be sufficient. In her September 2010 Washington Post article, "Agencies Aim to Bolster Cybersecurity", Ellen Nakashima outlined some of the up and coming practical problems associated with protecting the Country from cyber attack. She reported that the White House was investigating the thorny issue of the role of the Federal Government in protecting the Nation's critical infrastructure against cyber attacks since any attack by an adversary on the nation's power grid or other critical infrastructure would mean they would likely "shut down". Currently, Cyber Command is tasked only with protecting military computer networks. However, the entity charged with assisting the private sector - The Department of Homeland Security, lags behind the Defense Department in personnel, resources, and capabilities.

These and other issues will only be magnified as the nature and danger associated with Computer security issues crystalize over the next few years.

II. THE DEFENSE FOCUS: ON THE COMPUTER

Regardless of the type of computer crime, the defense focus is always the same: the computer itself. You must remember that the computer is the instrument that was allegedly used to commit the offense. When you encounter a computer crime, I recommend that you begin by ascertaining five items. Specifically, you should determine the following, to-wit:

- **HOW**
  How was the computer used? (What crime was allegedly committed?)
- **WHEN**
  When was the computer used? (What was the time span? What was the date of offense? Statute of limitations issue? Correct charging statute?)
- **WHERE**
  Where was the computer located? (Business, home, library, military base, etc. Does the court have jurisdiction?)
- **WHO**
  Who used the computer? (Can the prosecutor prove identity? Can they affirmatively link the defendant to the keyboard?)
- **WAS**
  Was the search and seizure of the computer conducted in a lawful manner?

Further, when you encounter a computer crime, regardless of the type, it is critical that you read the applicable federal or state statute. You must determine the elements of the alleged offense. Ask yourself, "How is the prosecutor

going to prove each and every element in this case?" Stand in the shoes of the prosecutor. Identify the weaknesses in his case as to the facts and elements of the offense.

III. UNAUTHORIZED COMPUTER ACCESS (Intruders/Hackers)

A. 18 U.S.C. § 1030

The explosive growth of the Internet has resulted in information becoming an increasingly valuable commodity. Several labels have been applied to the individuals who break into other's computer systems. Terms such as hacker, cracker, and intruder are commonly used; however, each term can have a different meaning. For example, **"hacker"** is often used to denote thrill seekers who break into other computer systems. When these individuals are caught they typically explain that they were motivated by their desire to improve computer security. Regardless of their motivation, hackers typically broadcast their conquest via BBSs. These communications often include the log-on and password for the newly compromised system. **"Crackers"**,on the other hand, are commonly defined as being more interested in breaking into a computer system to perform acts of vandalism. The term **"intruder"** in this paper includes hackers and crackers.

The main anti-intruder law is 18 U.S.C. § 1030. This statute was first enacted as the "Computer Fraud and Abuse Act of 1996." Effective October 26, 2001, Congress modified the 1996 Act. The most significant changes were: (1) increasing penalties for hackers who damage computers; (2) clarifying the intent element of such crimes; and (3) providing that damage caused to separate computers can be aggregated for purposes of satisfying the statute's jurisdictional threshold.

As presently written, 18 U.S.C. § 1030 creates six felony offenses and five misdemeanors.

Example violations of section 1030 would include:

- Hacking into a protected computer to steal information
- Destroying data or damaging hardware on protected computers by transmitting commands (e.g. virus or worm)
- "Denial of Service" attacks against protected computer
- Extortion based on threat to crash protected computer
- Attempts are also covered, under 1030(b)

18 U.S.C. § 1030(a)(1) punishes the act of obtaining national security information without or in excess of authorization and then willfully providing or attempting to provide the information to an unauthorized recipient, or willfully retaining the information. Investigating or indicting a case under section 1030(a)(1) require the prior approval of the National Security Division of the Department of Justice, through the Counterespionage Section.

18 U.S.C. § 1030(a)(2) prohibits unlawful access to confidential data or information. A violation of this subsection is misdemeanor with a punishment range of not more than one year imprisonment and/or a $100,000 fine. However, if this offense was committed for purposes of commercial advantage or private financial gain, and the value of the information obtained exceeds $5,000, the offense becomes a felony with a penalty range of not more than five years imprisonment and/or a $250,000 fine. 18 U.S.C. § 1030(c)(2)(B).

On November 5, 2003, a federal grand jury in Dallas, TX, returned a ten-count indictment against an employee of the Federal Bureau of Investigation for allegedly misusing agency computers to access FBI investigation files and then disclosing the information to friends and family. *United States v. Fudge*, N.D. Texas, No. 3:03CR380, 11/5/03.

The indictment charged Jeffrey D. Fudge with misusing his position of trust as an FBI investigative analyst. The charges include eight counts of exceeding authorized access to a government computer, a violation of 18 U.S.C. § 1030(a)(2)(B)&(C) and (c)(2)(B)(ii). Fudge entered into a plea agreement and received two years' probation.

Section 1030(a)(3) protects against "trespasses" by outsiders into federal government computers, even when no information is obtained during such trespasses. Congress limited this section's application to outsiders out of concern that federal employees could become unwittingly subject to prosecution or punished criminally when administrative sanctions were more appropriate. Congress, however, intended *inter*departmental trespasses (rather than *intra*departmental trespasses) to be punishable under section 1030(a)(3).

Section 1030(a)(4) establishes the offense of computer fraud. It requires that the government prove that, in furthering an intended fraud, the accused knowingly accessed without proper authorization a protected computer and obtained something of value. If the only thing obtained is the use of the computer the value of such use must

have exceeded $5,000 in any one-year period. The $5,000 figure was designed to limit the application of this felony to the more serious offenders and was generally tailored to protect "supercomputers." This section targets both outsiders and insiders, and provides for a maximum sentence of not more than five years imprisonment.

On January 12, 2004, a hacker broke in to the computer network of the University of Missouri-Kansas City and downloaded a file containing user names and passwords for some 17,000 e-mail accounts. The incident prompted officials immediately to shut down the network's link to the Internet, and to ask users later that day to change their passwords. The university also contacted the Federal Bureau of Investigation, which began a probe.

Section 1030(a)(5) is probably the most commonly prosecuted "hacking" subsection. Section 1030(a)(5) was enacted in response to the Morris Internet Worm. In United States v. Morris, 928 F.2d 504 (2nd Cir. 1991)a college student set loose a program (worm) on the Internet that crippled over 6,000 educational, medical, and military computer systems. The 2001 Act made several important clarifications to this section of 1030.

Under 1030(a)(5)(A)(I), an offense is committed if a person "knowingly causes the transmission of a program, code, information, or command to a protected computer" and intentionally causes damage. Section 1030(a)(5)(A)(ii) criminalizes accessing without authorization a protected computer and recklessly causing damage. Section 1030(a)(5)(A)(iii) criminalizes intentionally accessing a protected computer and causing damage. A chart outlining many of the federal cases prosecuted under § 1030 to date can be found online at the following URL, www.cybercrime.gov/cccases.html.

On August 29, 2003, federal investigators arrested an 18-year-old for releasing a dangerous form of the so-called "Blaster" worm. Jeffrey Lee Parson was charged with knowingly developing and releasing onto the Internet the Blaster computer worm, which infected at least 7,000 individual Internet users' computers.

"The Blaster computer worm and its variants wreaked havoc on the Internet, and cost businesses and computer users substantial time and money," then-Attorney General John Ashcroft said in a statement. "The Department of Justice takes these crimes very seriously, and we will devote every resource possible to tracking down those who seek to attack our technological infrastructure."

Parson was sentenced in January 2005 to an 18-month sentence and ten months' community service. Parson has served his time at a minimum security prison. Scheduled for release in January 2008, he faces three years of supervised release after his term, during which he can use computers only for business or education.

The 2001 Act increased the punishment for a violation of § 1030(a)(5)(A)(I) – intentionally causing damage – from not more than five years imprisonment to not more than ten years imprisonment and/or a $250,000 fine. The punishment for a violation of § 1030(a)(5)(A)(ii) – recklessly causing damaging – is not more than five years imprisonment and/or a $250,000 fine. A second violation (including a violation after a prior felony conviction for a state computer hacking crime) carries a more severe maximum punishment. See 18 U.S.C. §§ 1030(c)&(e)(10). A violation of § 1030(a)(5)(A)(iii) – causing damage – carries only a misdemeanor level of punishment. 18 U.S.C. § 1030(c)(2)(A).

Note: The 2002 Cyber Security Enhancement Act increases penalties for those who "knowingly or recklessly" cause or attempt to cause death or serious injury through a cyberattack, in violation of Section 1030(a)(5)(A)(I).

"Protected computer" is broadly defined in § 1030(e)(2) of the statute. Essentially, there are three groups of protected computers: 1) any computer that is "exclusively for the use of a financial institution or the United States Government;" 2) any computer that is used part-time by a financial institution or the United States Government, if the offense affects that use; or 3) any computer "which is used in interstate or foreign commerce of communication." This last group might include **any** computer connected to the Internet. Computers in foreign countries are now included in the new expanded 2001 Act definition.

Note: The U.S. District Court for the Western District of Louisiana decided that a personal computer used by a work-at-home employee for company business was a "protected computer" within the meaning of the federal Computer Fraud and Abuse Act.(*U.S. GreenFiber v. Brooks*, W.D. La., No. 02-2215, 10/25/02). The court went on to hold that the employee's act of deleting business-related files from the computer before she returned it to the company, after her termination, was an unauthorized access of the computer, in violation of the CFAA.

The new definition of "damages" in § 1030 does not include a reference to loss amount. "Damage" is now defined in 18 U.S.C. § 1030 (e)(8) as "any impairment to the integrity or availability of data, a program, a system, or information." Under this definition, the government need not prove that the defendant intended to cause $5,000 worth of damage. Rather, the government must prove one of the requisite *mens rea* with respect to causing damage and then must establish that the damage caused was $5,000 or greater, or falls within one of the other statutorily defined categories qualifying as damage. See 18 U.S.C. § 1030(a)(5)(B).

In United States v. Middleton, 231 F.3d 1207 (9th Cir. 2000) (analyzing the previous version of § 1030), the Ninth Circuit found that "damage" includes any loss that was a foreseeable consequence of the criminal conduct, including costs necessary to "resecure" the computers. The Court further held that the government could prove the $5,000 amount by putting on evidence of the hourly wage of the victim company's employees and the number of hours they spent to fix the computer problem. Id. at 1214. The broad definition of "loss" used in Middleton was adopted by Congress in the new 2001 law. "Loss" is defined in 1030(e)(11) as:

> any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

The 2001 Act also provides that the government may aggregate "loss resulting from related course of conduct affecting 1 or more other protected computers," which occurs to one or more persons during a one year period. 18 U.S.C. § 1030(a)(5)(B). Note that there is not a loss minimum if the computer is "used by or for a government entity in furtherance of the administration of justice, national defense, or national security." 18 U.S.C. § 1030(a)(5)(B)(v).

18 U.S.C. § 1030(a)(6) prohibits trafficking in computer passwords. The "Access Device Fraud Act" at 18 U.S.C. § 1029 prohibits both trafficking and possession of unauthorized computer passwords. §1030(a)(6) establishes trafficking in computer passwords as a misdemeanor and requires that the government prove:

1) that the accused knowingly obtained and transferred or disposed of passwords to another;
2) that the accused did so with the intent to defraud; and
3) that this conduct affected interstate or foreign commerce or that the computer is used by the United States Government.

Although "password" is not defined in 18 U.S.C. § 1030 or the main statute dealing with passwords, 18 U.S.C. § 1029, the Senate Committee defined password to include "a set of instructions or directions for gaining access to a computer." The Committee indicated that the password was to be broadly construed to cover more than a single word. (See S. Rep. No. 432, 99th cong., 2d Sess.9 (1986).)

18 U.S.C. § 1030(a)(7) prohibits computer extortion, which carries up to five years imprisonment and fine for the first offense. The elements of this offense are:

1) to transmit in interstate or foreign commerce a communication that contains a threat to cause damage to a protected computer; and
2) that the threat is made with the intent to extort money or other thing of value from any person or entity.

This section was enacted in response to actual cases where intruders would break into others' computer systems and encrypt their data so that the computer system was rendered inoperable and then demand money for the key to unencrypt the information.

B. Sentencing Guidelines for § 1030 Violations

The Sentencing Guideline in 2B1.1(b)(1) addresses the harm and invasion of privacy that can result from offenses involving the misuse of, or damage to, computers. *The applicable loss of each case is calculated under 2B1.1(b)(1).* The Guidelines implement the directive in section 225(b) of the Homeland Security Act of 2002, which required the Commission to review, and if appropriate amend, the guidelines and policy statements applicable to persons convicted of

offenses under 18 U.S.C. § 1030.

This provision of the guidelines adds new specific offense characteristic at § 2B1.1(b)(15) with three alternative enhancements of two, four, and six levels.

Second, the amendment modifies the rule of construction relating to the calculation of loss in protected computer cases. This change was made to incorporate more fully the statutory definition of loss at 18 U.S.C. § 1030(e)(11), added as part of the USA PATRIOT Act, and to clarify its application to all 18 U.S.C. § 1030 offenses sentenced under § 2B1.1.

Third, the amendment expands the upward departure note in § 2B1.1. That note provides that an upward departure may be warranted if an offense caused or risked substantial non-monetary harm, including physical harm. The amendment adds a provision that expressly states that an upward departure would be warranted for an offense under 18 U.S.C. § 1030 involving damage to a protected computer that results in death.

Fourth, the amendment modifies § 2B2.3, to which 18 U.S.C. § 1030(a)(3) (misdemeanor trespass on a government computer) offenses are referenced, and § 2B3.2, to which 18 U.S.C. § 1030(a)(7) (extortionate demand to damage protected computer) offenses are referenced, to provide enhancement relating to computer systems used to maintain or operate a critical infrastructure, or by or for a government entity in furtherance of the administration of justice, national defense, or national security.

Finally, the amendment references offenses under 18 U.S.C. § 2701 (unlawful access to stored communications) to § 2B1.1.

C. Remote Access Tools or "RAT"

For years, office IT personnel have used a remote access tool, or "RAT" to literally "take over" a machine within their company and, in turn, fix problems with employee's computers. remotely. It's an efficient way to solve computer problems without every having to leave their desks. Such applications are routinely used by computer companies' tech support operations to effect remote repairs or modifications to customer's computers and are generally extraordinarily helpful, productive, and benign in their uses. Until they're not.

However, hackers have discovered that RAT's can also be used for illicit purposes as well and can be a boon to those seeking to profit from unlawful access of the machines of others. All it would take would be to (1) create a RAT, (2) create a "user friendly" interface, and (3) market the application and sell it to any novice purchaser who intend to use it for illegal purposes.

D. "Blackshades"

Monday, May 19, 2014, more than 90 people in 19 Countries were arrested for use and distribution of malicious software called "Blackshade" that infected more than 500,000 computers.

"Blackshades" is an example of one such "Remote Access Tool" or RAT. Blackshades targets Microsoft Windows-based operating systems and allows cybercriminals to take control of a computer from a remote location. Once inside, they can spy on you through your web camera, steal your files and account information, encrypt and hold your data for ransom, and see what you are typing - including the keystrokes used for a user's passwords.

Perhaps the most sobering notion is the fact that this RAT doesn't require the user to be in any way sophisticated to effect real havoc on a target. Blackshades was available via Pay Pal for $40 and the interface of the tool was so intuitive that almost anyone could use it.

24 year old Swedish man Alex Yucel was arrested along with his partner in crime, Michael Hogue for having created and marketed the malware.

Its improper uses included "sextortion" where the user would capture nude pictures of a computer's user by remotely activating the computer's camera, then require payment or further sexual performance in lieu of online dissemination of the previously captured illicit images. This is the scam used on Miss Teen U.S.A. Cassidy Wolf. In her case, 20 year old Jared Abramson was captured and prosecuted and received 18 months in prison for performing the scam.

The Government has posted a link to some tell tale signs of a "Blackshades" infection at the following link:
http://www.fbi.gov/news/stories/2014/may/international-blackshades-malware-takedown/could-your-computer-be-infected-by-blackshades

E. Hackers Defense: The Trojan Horse

Prosecutors have come across a legal defense expected to become widespread in an era of hijacked PCs and laptops: the Trojan Horse

Defense.

In one case that was being watched by computer security experts, Aaron Caffrey, 19, was acquitted in October 2003 in the United Kingdom on charges of hacking into the computer system of the Houston Pilots, an independent contractor for the Port of Houston, in September 2001.

Caffrey had been charged with breaking into the system and crippling the server that provides scheduling information for all ships entering the world's sixth-largest port.

Although authorities traced the hack back to Caffrey's computer, his attorneys successfully argued that someone must have remotely planted a program, called a "trojan," onto his computer that did the hacking and that could have been programmed to self-destruct

In two other cases, British men were accused of downloading child pornography but their attorneys successfully argued that trojan programs found on their computers were to blame.

Some legal and security experts say the trojan defense is a valid one because computer hijacking occurs all the time and hackers can easily cover their tracks.

"I've seen cases where there is a similar defense and it could work or not work based on corroborating evidence: such as how technical the defendant is, said Jennifer Stisa Granick, clinical director of the Sanford Law Center for Internet and Society.

It is relatively easy to trace a hack back to a particular computer, but proving that a specific person committed the crime is much more difficult, she said.

Someone other than the computer owner could use the machine, either by gaining physical access or remotely installing trojan software that was slipped onto the computer via an e-mail sent to the computer owner or downloaded from a malicious Web site, they said.

The defense is likely to become more widespread especially given the increasing use of "spyware" programs that can be used by hackers to steal passwords and essentially eavesdrop an a computer user, experts said.

"The emergence of spyware will only enhance these claims," said Michael Geist, a law professor at the University of Ottawa Law School in Canada. "We're going to have to sort though the level of responsibility a person has for operating their own computer."

F. Spyware Programs

Software programs that surreptitiously enter personal computers have grown in recent years, and while many are not clearly illegal, they pose cybersecurity and privacy challenges that require government, industry, and consumers to respond, according to a report released on November 18, 2003, by the Center for Democracy and Technology (CDT).

A wide range of "spyware" programs exist today, complicating legal and regulatory solutions. Those programs include "snoopware" and "trespassware."

"Snoopware" includes programs surreptitiously installed by a third party that track keystrokes and web sites visited, or capture passwords and other information and pass them back to the third party.

"Trespassware" includes adware and other applications bundled with desired software, which deliver advertisements or otherwise hijack a user's computer without collecting information on the user. Such programs exist in a legal gray zone, CDT said.

"Snoopware" poses severe privacy risks, but it also appears to be relatively uncommon. Of primary concern to CDT is trespassware, which appears to be far more common, based on complaints posted on the Web.

"Trespassware" programs sometimes hobble computer performance, prompting users to mistakenly call software or ISP help desks, unaware of the hidden program causing the problem. In addition, the programs are notoriously difficult to remove, remaining even when the host program with which it entered a computer is uninstalled.

For example, a company calling itself Lover Spy has begun offering a way for jealous lovers to spy on the computer activity of their maters by sending an electronic greeting, that doubles as a bugging device. Computer security experts have said that the Lover Spy service and software appear to violate U.S. law, but also said the surveillance program pointed to an increasingly common way for hackers to seize control of computers.

Marketed as a way to "catch a cheating lover," the Lover Spy company offers to send an e-mail greeting card to lure the victim to a Web site that will download onto the victim's computer a trojan program to be used for spying.

The Lover Spy software, purports to record anything the victim does on the computer, including all keystrokes, passwords, e-mail, chats and screen shots and even turn on the victim's Web camera.

The spy program discreetly sends the

information to the Lover Spy server which then forwards it on to whoever paid for the software, maintaining their anonymity.

"You don't need physical access to the computer," said Richard Smith, and independent privacy and security researcher in Boston. "It makes it so you can spy on anybody you want."

"That would be a felony," said Mark Rasch, former head of the U.S. Department of Justice's computer crime unit and chief security counsel for security company Solutionary. "Loading a program onto someone else's computer without their authorization is patently illegal."

"That is clearly a wiretapping violation," Chris Hoofnagle, associate director of the Electronic Privacy Information Center, said when told of Lover Spy.

In August 2005, the U.S. Attorney's office for the Southern District of California announced the indictment of Carlos Enrique Perez-Melara, the creator of "Loverspy". He was named in a 35-count indictment and charged with creating a surreptitious interception device (i.e. the Loverspy program); sending the program concealed in an electronic greeting card to victims; advertising the program; advertising the surreptitious use of the program; illegal wiretapping; disclosing illegally intercepted communications; and obtaining unauthorized access to the victim's computers. Each count of the 35-count indictment carries a maximum penalty of five years in prison and a maximum fine of $250,000 per count. Four other individuals who used Loverspy to break into computers and intercept the communications of others were also indicted in separate two-count indictments, in which they were charged with illegal computer hacking through the utilization of Loverspy. To date, the indictment against Perez-Malara is pending but there has been no action on the case for several years since, as of May 2014, Perez-Melara remains on the run and remains on the F.B.I.'s Most Wanted list with El Salvador being his last known location. The four purchasers were prosecuted separate. Each entered into a plea agreement and received a probationary type of sentence. Other Loverspy purchasers have been prosecuted by federal authorities in Charlotte, N.C., Dallas, TX, and Honolulu, HI.

IV. ILLEGAL CAPTURE, TRAFFICKING, AND POSSESSION OF COMPUTER ACCESS DEVICES AND PASSWORDS, 18 U.S.C. § 1029 and 18 U.S.C. § 1030.

18 U.S.C. § 1029 prohibits trafficking and possession of unauthorized computer passwords. While the majority of this statute is directed at credit card and cellular phone fraud, the term "access devices" has been interpreted to include computer passwords. In United States v. Fernandez, 1993 U.S. Dist. LEXIS 3590 (1993) (not published), the court held that "the plain meaning of the statute certainly covers stolen and fraudulently obtained passwords which may be used to access computers to wrongfully obtain things of value, such as telephone and credit services." 1993 U.S. Dist. LEXIS 3590, at *6.

The statute makes it a felony for an individual who, knowingly and with intent to defraud, possesses, traffics, or uses an unauthorized or counterfeit access device; or produces, traffics in, has control or custody of, or possesses device making equipment. There are numerous sections to this statute and the requirements of proof vary among them.

Section 1029(a)(3) prohibits a person from knowingly, and with the intent to defraud, possessing fifteen or more devices, which are counterfeit or unauthorized access devices. Intruders frequently collect and trade password information on systems they have compromised. Possession of such passwords provides verification that the intruder has gained access to various computer systems and is often used for bragging rights. Intruders frequently install "sniffers" so that they can collect additional passwords. A sniffer, which is a software program that intruders secrete on a compromised computer system, records the log-on name and passwords of valid users. Intruders retrieve and use this information to masquerade as the valid user. If a sniffer is placed on a large computer network, it can collect literally hundreds of passwords. Use of such an illegally placed sniffer could constitute a felony violation of the Wiretap Act.

One § 1029(a)(3) case is *U.S. v. Fitzgerald*, N.D. Cal., No. CR-02-0406, 2003.

Shawn Webb Fitzgerald was indicted on charges of possessing unauthorized access devices and possession of counterfeit mail keys. Fitzgerald was accused of stealing mail around the San Francisco Bay Area from December 2001 through April 2002.

In the plea agreement, Fitzgerald admitted stealing bank statements with checking account numbers and related information; credit card statements with account numbers; stock brokerage statements with account information; and other materials.

Prosecutors accused Fitzgerald of possessing 15 or more credit cards, bank and brokerage account number, electronic serial numbers, or other means of account access. He pled guilty to two counts of violating 18 U.S.C. § 1029(a)(3). He received 105 months in prison.

Another intruder trick is to download or copy the password file from a targeted computer system. This file is designed to hold all of the authorized users' passwords in one central repository. For security reasons the passwords are automatically encrypted and maintained in the file in this encrypted state. Unfortunately, there are a number of software programs such as "Crack" that will decrypt these password files. These cracking programs are readily and freely available over the Internet.

Japanese police arrested two cyberburglars who withdrew $150,000 from third-party accounts by installing an ID/password recording application call the Key Logger on Internet café computers on March 11, 2003. The Key Logger, which records vital information such as IDs and passwords, at more than a dozen Internet cafés in Tokyo since about two years ago and visited the cafés every few weeks and collected third-party IDs and passwords.

They were keeping as many as 720 IDs and passwords of bank accounts and credit cards of third parties, as well as 195 IDs and passwords of women who frequented the Internet cafés, police said.

As noted in Section III above, § 1030(a)(6) criminalizes trafficking, with the intent to defraud, in passwords "or other similar information through which a computer may be accessed" if such trafficking affects interstate commerce or the computer is used by or for the United States government. A first offense is a misdemeanor and a subsequent offense is a felony.

Current Trends in Access Device Fraud

Perhaps of greatest interest to average consumers is the outbreak of high-tech methods by which criminals obtain credit card and debit card information from unsuspecting account holders who are otherwise properly using their "devices" (debit/credit cards) for their own convenience.

The unscrupulous have become increasingly efficient in their efforts to unlawfully obtain credit/debit card information this information by essentially turning technology around and using it to facilitate its attack on itself.

The use of "skimmers" is on the rise as the information from a magnetic card is captured through the use a device designed and used to intercept the information as the card user inserts the card into the "slot" while using it. The criminals insert a piece of hardware that fits either just inside or just outside the proper slot and which often appears to be part of the machine. The information is then captured for use later where it's placed on readily available blank magnetic cards and then sold into the black market

The important issue to be aware of in this genre' of offenses is that, while the credit card holder is often protected, debit card holders are rarely protected from loss and many victims can be wiped out in short order by experienced thieves who are able to access and take moneys oftentimes before the victim is even aware.

The theft of this information is not restricted to cards with the magnetic strips either. The cards containing the radio frequency technology are now being compromised by individuals armed with nothing more than a radio controlled reader walking up to someone in a crowded venue such as an airport, bus terminal, or sporting event.

The ultimate conclusion is that, in the current cycle, criminals have caught up with the technology and the dynamic is likely to change only when the cost of modernization of the current U.S. system becomes less than the losses felt by the industry.

In Europe, the issue is less predominant in that the magnetic cards have become essentially obsolete and most, if not all, magnetic cards remaining are scheduled in the near future for discontinued acceptance within the next 2-4 years.

V. IDENTITY THEFT, 18 U.S.C. § 1028

The Federal Trade Commission announced on December 23, 2005 that it currently records about 3,231 complaints and inquiries per week on identity theft, compared with 1,700 in March of 2002. The report stated identity theft was the number one consumer complaint during 2005 and attributed much of the increase to advanced technology, especially the Internet.

A Federal Trade Commission site has been constructed solely for the dissemination of information related to prevention and planning for Identity Theft and can be found at http://www.ftc.gov/bcp/edu/ microsites/idtheft/ . The Federal trade Commission's side is http://www.ftc.gov/ and the Consumer Response Center is at Room 130, 600 Pennsylvania Ave. NW, Washington, DC, 20580; (202) 382-4357.

A provision of the Fair and Accurate Credit Transactions Act took effect December 1, 2004, giving residents of the western part of the United States the right to a free copy of their credit report each year. The provision will be phased in for consumers in states east of the Rocky Mountains over the course of the next nine months.

Title 18, U.S.C. § 1028, The Identity Theft and Assumption Deterrence Act, was enacted October 30, 1998. This statute essentially creates a new crime – Identity Theft – which recognizes that computers can be used to create documents that allow a user to assume the identity of another or even create fraudulent identities. This practice has already resulted in considerable monetary loss to businesses and financial institutions and can have profound and long-lasting effects on the victim's credit rating.

The statutory penalty provisions vary depending on the type of identification used, produced, or obtained and the number of identification documents involved in the offense. 18 U.S.C. § 1028(b). The U.S. Sentencing Commission on May 1, 2000, sent to Congress several amendments to the federal sentencing guidelines that significantly increased penalties for a number of computer crimes. See U.S.S.G § 2B1.1(b)(9).

The Sentencing Commission voted to increase penalties for criminals who steal another person's means of identification and then use that stolen document to commit additional crimes, such as obtaining fraudulent loans or credit cards. In so doing, the Commission recognized that the individual whose identity is stolen is also a victim of the fraud, just as is the bank or credit card company. In the same amendment, the Commission also increased penalties for the cloning of wireless telephones in response to the Wireless Telephone Protection Act of 1998.

The Identity Theft Penalty Enhancement Act, which took effect July 15, 2004, established a new offense of aggravated identity theft. Section 1028A adds an additional two year term of imprisonment in cases where a defendant "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person" during and in relation to any felony violation of certain enumerated federal offenses, including 18 U.S.C. §§ 1028 (but not 1028 (a)(7)), 1029, 1030, 1037, and 1343. See 18 U.S.C. § 1028A(a)(1). In cases of terrorism-related aggravated identity theft, including that related to section 1030(a)(1), that section imposes an additional five-year term of imprisonment. 18 U.S.C. § 1028A(a)(2). In most cases, the additional terms of imprisonment will run consecutively, not concurrently. 18 U.S.C. § 1028 A (b).

On May 20, 2000, a 23-year old convicted felon told a Senate panel how he created phony documents using a computer at a public library and public government records online.

"The availability of false identification on the Internet is a ... growing problem, to which we plan to devote additional resources and attention," Secret Service Director Brian Stafford testified before the Senate Governmental Affairs Committee's investigative subcommittee.

There are three levels of fake ID procurement that subcommittee investigators found in a five-month undercover inquiry.

First, some Web sites sell bogus, real-looking documents in the customer's name. Others sell high-quality computer files, called templates, that allow customers to make their own phony documents.

The false documents offered on some sites are of "shockingly high quality," K. Lee Blalack II, the panel's chief counsel and staff director, testified at the hearing.

The fake IDs often contain holograms, bar codes, magnetic stripes, and other security features added to genuine documents to prevent counterfeiting.

On July 24, 2001, the FTC settled with an individual who had sold internet access to software used to make false identity documents. Templates and software were used to produce fake drivers licenses for California, Georgia, Florida, Maine, Nevada, New Hampshire, New Jersey, Utah, Wisconsin, and New York.

The web site sold 45 days of access to the templates for $29.99. The site also provided access to birth certificate templates, programs to create bar codes, and a program to falsify Social Security numbers. Federal Trade Commission v. Martinez, C.D. Cal., No. 00-12701-CAS 7/24/01.

On January 6, 2003, six firms that used the Internet to sell driver's permits were selling worthless documents to unsuspecting consumers, according to charges filed by the Federal Trade Commission as part of "Operation License for Trouble," and enforcement sweep targeting sellers of bogus documents. *Federal Trade Commission v. Carlton Press Inc.*, S.D.N.Y., No. 03-CV-0226-RLC, 1/16/03.

A federal jury in Los Angeles on December 4, 2003, found a former Global Crossing computer technician, Steven William Sutcliffe, guilty of eight felony counts related to a web site where he posted Social Security numbers and other personal

information of thousands of Global Crossing employees. *U.S. v. Sutcliffe,* C.D. Cal., No. CR 02-350(A)-AHM, 12/4/03. It may be the first conviction under the federal statute, 18 U.S.C. § 1028(a)(7), prohibiting online posting of Social Security numbers with the intent to aid and abet identity theft. Mr. Sutcliffe received a four-year sentence. His conviction and sentence were affirmed in *U.S. v. Sutcliffe*, 505 F.3d 944 (9th Cir. 2007).

The San Diego County District Attorney on November 18, 2003, announced a 154-count indictment, naming 21 defendants for identity theft-related crimes, making it the largest identity theft ring ever prosecuted in the county. *California v. Ramirez*, Cal. Super. Ct., No. SCD160792, *indictment* 10/31/03. One of the lead defendants, was enlisted in the U.S. Navy and had a position that gave her access to Navy personnel records.

On November 22, 2004, Nineteen (19) individuals were indicted and were alleged to have founded, moderated and operated "www.shadowcrew.com" – one the largest illegal online centers for trafficking in stolen identity information and documents, as well as stolen credit and debit card numbers.

The 62-count indictment, returned by a federal grand jury in Newark, New Jersey, alleged that the 19 individuals from across the United States and in several foreign countries conspired with others to operate "Shadowcrew," a website with approximately 4,000 members that was dedicated to facilitating malicious computer hacking and the dissemination of stolen credit card, debit card and bank account numbers and counterfeit identification documents, such as drivers' license, passports and Social Security cards. The indictment alleges a conspiracy to commit activity after referred to as "carding" – the use of account numbers and counterfeit identity documents to complete identity theft and defraud banks and retailers. Shadowcrew members allegedly trafficked in at least 1.7 million stolen credit card numbers and caused total losses in excess of $4 million dollars. Albert Gonzalez was known as "CumbaJohnny," and he was an administrator of Shadowcrew. He cooperated with the Secret Service as an informant, and allowed federal agents to watch his conduct on the Shadowcrew site, which led to the then-largest US roundup of identity thieves in 2004. Gonzalez himself was never charged. Gonzalez, however, did not stop his criminal activities.

Operating from a Miami base, he found new accomplices and drove highways looking for improperly secured wireless networks inside retailers. Once inside the networks, his crew installed "sniffers" to monitor traffic. The same ring was responsible for a massive breach at T.J. Maxx owner TJX Cos. and the lifting of bank account PINs from Citibank-branded ATMs inside 7-Eleven stores.

Gonzalez was charged in three separate federal indictments: May 2008 in New York for the Dave & Busters case (*U.S. v. Yastremsky*, 08-CR-00160).); May 2008 in Massachusetts for the TJ Maxx case (*U.S. v. Gonzales*, 08-CR-10223) ; August 2009 in New Jersey in connection with the Heartland Payment case. On December 28, 2009, Gonzalez entered a guilty plea to the Massachusetts conspiracy charges in the largest known identity theft case to date. On march 25, 2010, Gonzalez was sentenced to 20 years in Federal Prison and assessed a $25,000 fine. Mr Gonzalez formally entered the plea in the U.S. District Court in Boston in a case brought over the penetration of multiple retail chains and Heartland Payment Systems, a credit card and debit card processor that prosecutors said jeopardized millions of accounts.

In *United States v. Flores-Figueroa*, 129 U.S. 1886 (May 2009), the Supreme Court reversed a conviction under 18 U.S.C. 1028 (a)(1). Ignacio Flores-Figueroa, a citizen of Mexico gave his employer a false name, birth date, and Social Security number, along with a counterfeit alien registration card in order to secure employment. The Social Security number and the number on the alien registration card were not those of a real person. In 2006, Flores presented his employer with new counterfeit Social Security and alien registration cards; these cards (unlike Flores' old alien registration card) used his real name. But this time the numbers on both cards were in fact numbers assigned to other people. Flores' employer reported his request to U.S. Immigration and Customs Enforcement. Customs discovered that the numbers on Flores' new documents belonged to other people. The United States then charged Flores with two predicate crimes, namely, entering the United States without inspection, 8 U.S.C. § 1325(a), and misusing immigration documents, 18 U.S.C. § 1546(a). It also charged him with aggravated identity theft, 18 U.S.C. 1028A(a)(1), the crime at issue in the case before the Supreme Court.

The Court stated, "The question is whether the statute requires the Government to show that the defendant *knew* that the "means of identification" he or she unlawfully transferred, possessed, or used, in fact, belonged to "another person." We

conclude that it does . ”

VI. CYBERSTALKING

A. What Is Cyberstalking?

There is no universally accepted definition of cyberstalking. The term is normally used to refer to the use of the Internet, e-mail, or other electronic communications devices to stalk another person. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person’s home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person’s property.

A cyberstalker may send repeated, threatening, or harassing messages by the simple push of a button; more sophisticated cyberstalkers use programs to send messages at regular or random intervals without being physically present at the computer terminal.

A cyberstalker’s true identity can be concealed by using different ISPs and/or by adopting different screen names. More experienced stalkers can use anonymous remailers that make it all-but-impossible to determine the true identity of the source of an e-mail or other electronic communication. A number of law enforcement agencies report they currently are confronting cyberstalking cases involving the use of anonymous remailers.

Anonymity leaves the cyberstalker in an advantageous position. Unbeknownst to the target, the perpetrator could be in another state, around the corner, or in the next cubicle at work. The perpetrator could be a former friend or lover, a total stranger met in a chat room, or simply a teenager playing a practical joke. The veil of anonymity often encourages the perpetrator to continue these acts.

Los Angeles and New York, have both seen numerous incidents of cyberstalking and have specialized units available to investigate and prosecute these cases. For example, Los Angeles has developed the Stalking and Threat Assessment Team. Similarly, the New York City Police Department created the Computer Investigation and Technology Unit.

B. Federal Cyberstalking Laws

Under 18 U.S.C. 2261A, it is a federal crime, punishable by up to five years in prison and a fine of up to $250,000, to transmit any communication in interstate or foreign commerce containing a threat to injure the person of another. Section 875(c) applies to any communication actually transmitted in interstate or foreign commerce - thus it includes threats transmitted in interstate or foreign commerce via the telephone, e-mail, beepers, or the Internet.

Title 18 U.S.C. 2261A is not an all-purpose anti-cyberstalking statute. First, it applies only to communications of actual threats. Thus, it would not apply in a situation where a cyberstalker engaged in a pattern of conduct intended to harass or annoy another (absent some threat). Also, it is not clear that it would apply to situations where a person harasses or terrorizes another by posting messages on a bulletin board or in a chat room encouraging others to harass or annoy another person.

The Fifth Circuit considered one of the first Internet threat cases prosecuted under this statute. United States v. Morales, 272 F.3d 284 (5th Cir. 2001). Defendant high school student was convicted of making interstate threatening communication, based on Internet “chat room” conversation in which he threatened to kill fellow students. Defendant appealed. The Court of appeals, held that: (1) general-intent requirement of governing statute was satisfied since defendant admitted to sending threat in order to see how recipient would react; (2) question of whether message was “true threat” as opposed to political hyperbole was for jury; (3) fact that message was sent to third party rather than to fellow students did not preclude prosecution; and (4) government did not have to prove that defendant intended message to be threat, only that statement was made knowingly and intentionally. But see United States v. Baker, 890 F. Supp. 1375, 1390 (E.D. Mich. 1995) (granting defendant's motion to quash indictment against him for statements he made over the Internet because they were not true threats).

A California man was charged with making internet e-mail death threats against employees of a Canadian Internet advertising company. *United States v. Booher*, N.D. Cal., No. 03CR2017, *indictment* 11/25/03. Federal prosecutors allege Charles Booher, repeatedly made e-mail death threats, including threats of mayhem and bodily harm against workers at the British Columbia marketing firm. The charges against Mr. Booher were eventually dropped.

Certain forms of cyberstalking also may be prosecuted under 47 U.S.C. 223. One provision of this statute makes it a federal crime, punishable

by up to two years in prison, to use a telephone or telecommunications device to annoy, abuse, harass, or threaten any person at the called number. The statute also requires that the perpetrator not reveal his or her name. See 47 U.S.C. 223(a)(1)(C). Although this statute is broader than 18 U.S.C. 875 – in that it covers both threats and harassment – Section 223 applies only to direct communications between the perpetrator and the victim. Thus, it would not reach a cyberstalking situation where a person harasses or terrorizes another person by posting messages on a bulletin board or in a chat room encouraging others to harass or annoy another person. Moreover, Section 223 is only a misdemeanor, punishable by not more than two years in prison.

On November 22, 2004, James Robert Murphy, 38, of Columbia, South Carolina, was sentenced to 5 years of probation, 500 hours of community service, and more than $12,000 in restitution for two counts of Use of a Telecommunications Device (the Internet) with Intent to Annoy, Abuse, Threaten or Harass. Murphy was indicted for sending harassing e-mails to a Seattle residence and to employees of the City of Seattle. He pleaded guilty to two counts in June 2004 in violation of 47 U.S.C. 223. He is the first person to be convicted under the statute. Murphy hid his identity with special e-mail programs and created the "Anti Joelle Fan Club" (AJFC) and repeatedly sent threatening e-mails from this alleged group.

The Interstate Stalking Act, signed into law by President Clinton in 1996, makes it a crime for any person to travel across state lines with the intent to injure or harass another person and, in the course thereof, places that person or a member of that person's family in reasonable fear of death or serious bodily injury. See 18 U.S.C. 2261A. Although a number of serious stalking cases have been prosecuted under Section 2261A, the requirement that the stalker physically travel across state lines makes it largely inapplicable to cyberstalking cases.

On September 10, 2002, in United States v. Bowker, docket number 4:01-CR-441-ALL, N.D. Ohio, the defendant was convicted under § 2261A and sentenced to eight years in prison. Mr. Bowker sent obscene e-mails, made threatening telephone calls, and stole mail from the victim. The victim was a TV reporter in West Virginia; the defendant resided in Ohio.

The constitutionality of 2261A was upheld in the appeal of this same case in U.S. v. Bowker, 372 F.3d 365 (6th Cir. 2004). The appellant argued on appeal that the statute was unconstitutionally overbroad. The Sixth Circuit rejected these claims and wrote the following: "We fail to see how a law that prohibits interstate travel with the intent to kill, injure, harass or intimidate has a substantial sweep of constitutionally protected conduct. 18 U.S.C. § 2261A(1). The same is true with respect to the prohibition of intentionally using the internet in a course of conduct that places a person in reasonable fear of death or seriously bodily injury. 18 U.S.C. § 2261A(2). It is difficult to imagine what constitutionally-protected political or religious speech would fall under these statutory prohibitions. Most, if not all, of these laws' legal applications are to conduct that is not protected by the First Amendment. Thus, Bowker has failed to demonstrate how 18 U.S.C. § 2261A is substantially overbroad".

Finally, President Clinton signed a bill into law in October 1998 that protects children against online stalking. The statute, 18 U.S.C. 2425, makes it a federal crime to use any means of interstate or foreign commerce (such as a telephone line or the Internet) to knowingly communicate with any person with intent to solicit or entice a child into unlawful sexual activity. This new statute does not reach harassing phone calls to minors absent a showing of intent to entice or solicit the child for illicit sexual purposes.

VII. INTERNET FRAUD

A. Introduction

The Internet Fraud Complaint Center became the Internet Crime Complaint Center (IC3), under the control of the Federal Bureau of Investigation and National White Collar Crime Center (NW3C) in May of 2000.

The name change does not alter the mission of IC3 to receive, develop, and refer criminal complaints in the area of cybercrime, but was instituted to more accurately reflect the wider-ranging nature of online complaints being reported. The unit is a component of the FBI's Cyber Division and seeks to establish alliances between law enforcement as a whole, the 60 FBI-led cybercrime task forces, and private industry. On May 10, 2014, the IC3 received its 1 millionth complaint. This followed the receipt of 300,000 complaints per year for the previous 5 years. In 2013 alone, the verifiable dollar loss of complaints submitted to the IC3 totaled nearly

$800 million. The total dollar loss claimed from all complaints over the life of the IC3 exceeds $2 billion.

California, Florida, Texas, New York, and Pennsylvania were the top five states for victims of Internet fraud. In cases where the perpetrator had been identified, over three in four were male (???? did you mean three in four?) and over half resided in the states of California, New York, Florida, Texas, Illinois, Pennsylvania and Ohio.

To obtain a copy of IC3's latest Internet Crime Report, visit www.ic3.gov/mediaannualreports.aspx.

Recent high activity scams seen by IC3 include targeting of University employees and students, as well as phishing attacks targeting various telecommunication companies' customers. This is in addition to the always popular phishing emails to Super Bowl Tickets scams, phishing attempts associated with spoofed sites, re-shipping, eBay account takeovers, natural disaster fraud, and international lottery scams.

Operation E-CON and Cyber Sweep:

Examples of law enforcement operations undertaken in effort to ward off cyber crimes include E-CON in 2003 in which 135 people had been charged and more than $17 million seized in a crackdown on investment swindles, auction fraud, investment scams, and other forms of Internet fraud.

Those arrested stand accused of a variety of crimes, from setting up fake banking web sites to collect the account numbers of unsuspecting customers – to surreptitiously taping and selling unreleased movies, Ashcroft said.

Many of the cases involved advertising goods or services that did not exist. Defendants allegedly sold computers, video-game consoles, Beanie Babies, and other items though e-mail or online auction sites but never delivered them, while other allegedly sold counterfeit software and watches.

Operation Web Snare:

Another sign of the Justice Department's aggressive efforts to prosecute economic crimes committed on the Internet is "Operation Web Snare."

Operation Web Snare was the largest and most successful collaborative law-enforcement operation ever conducted to prosecute online fraud, stop identity theft, and prevent other computer-related crimes.

Between June 1st and August 26th, 2004, Operation Web Snare yielded more than 160 investigations in which more than 150,000 victims lost more than $215 million.

As a result of this operation, there were:

- More than 350 subjects of investigation;
- 53 convictions to date;
- A total of 117 criminal complaints, indictments, and informations; and
- The execution of more than 140 search and seizure warrants.

B. Online Drug Sales, Health Care, and Health Product Fraud

A federal prosecutor in Virginia on December 3, 2003, announced a 108-count indictment against 10 individuals and three companies for illegally selling prescription drugs through the Internet. *United States v. Chhabra*, E.D. Va., No. 03-530-A, *filed* 10/30/03.

The companies indicted are USA Prescription Chhabra Group LLC, and VKC Consulting LLC, all owned by Vineet Chhabra. Among the charges are that they sold Viagra and weight loss medications without following state and federal regulations. The charges included conspiring to unlawfully distribute and dispense Schedule III and IV controlled substances other than for medical purposes, and using a communication facility for distribution of the drugs. The indictment, which was returned by a federal grand jury in Alexandria, Va., charged not only the owners and operators of the web sites involved, but physicians and pharmacists as well. Vineet K. Chhabra entered his plea in U.S. District Court in Alexandria. That brought to seven the number of people who have pleaded guilty in the scheme that federal officials say illegally distributed millions of pills to Virginia, Maryland, the District and four other states. Chhabra was subsequently sentenced to a 33-month term of imprisonment.

Investigators are seeing more healthcare industry fraud schemes involving electronic fund transfers, in which criminals are hacking into government computer systems, changing addresses for providers, and then cashing insurers payments meant for providers, according to Tom Brennan, director of special investigations at Highmark Health Care.

Another "huge" problem for Highmark and other health care plans is pharmaceutical internet fraud. Certain controlled substances - in particular, Xanax, Vicodin, and Percocet - are being filled by dishonest pharmacists, who sell the drugs to addicts.

Improper Internet billing schemes are also increasing. One recent case involved a physician who billed an insurer for lesion removals. When the claims were analyzed, Brennan said it was clear that the physician was billing separately for lesion removals that should have been part of a single comprehensive service and was even billing services not rendered.

About 90 million Americans use the Internet to find health-related information, according to the Federal Trade Commission.

The FTC unveiled six enforcement actions on June 14, 2002, against companies that made fraudulent marketing claims for dietary supplements and other health products.

The targeted companies sold supplements, herbal products, and medical devices over the Internet that claimed to treat or cure cancer, HIV/AIDS, arthritis, hepatitis, Alzheimer's, diabetes, and other diseases, FTC Chairman Timothy Muris said at a press conference.

Although the enforcement actions targeted some of the most egregious health claims found on the Internet, many more companies are making unsubstantiated claims, he said. "FTC will step up its efforts to combat Internet health fraud."

C. Internet Auction Fraud

Internet auctions continue to be a source for fraudulent activities. Most online auction fraud cases are still prosecuted under the federal wire and mail fraud statutes. For example, On December 4, 2002, a Los Angeles man was charged with defrauding eBay buyers on six continents. Prosecutors are calling it one of the largest Internet auction scams yet uncovered. Chris Chong Kim, age 27, was charged with four counts of grand theft and 26 counts of hold a mock auction for allegedly failing to deliver the high-end computers and computer parts he sold on his eBay business site, Calvin Auctions. The online auction house received more than 170 complaints from customers around the world. Their losses ranged from $1,900 to $6,000 each, prosecutors said.

In 2004, the United State's Attorney's Office for the Northern District of California announced that Michael W. Gouveia was indicted for allegedly defrauding eBay users of thousands of dollars in auctions for rare Mickey Mantle and Michael Jordan sports cards.

According to the indictment, Mr. Gouveia defrauded eBay users of over $30,000 in connection with eBay auctions he hosted for collectible sports player cards. Mr. Gouveia was eventually sentenced to 8 months imprisonment, three years of Supervised Release, and was ordered to pay $34, 792.40 in restitution to his victims.

On August 1, 2003, the United States Court of Appeals for the Fourth Circuit, upheld the enhanced sentence imposed by the trial court against a West Virginia man convicted of defrauding customers in Internet auctions. United States v. Bell, 72 Fed. Appx. 25 (4th Cir. 2003). The court ruled that Vernon Derl Bell deserved a 15-month prison sentence for his fraud conviction under the federal sentencing guidelines as a "mass marketer" for defrauding 186 buyers on eBay out of more than $150,000. Bell conducted auctions for sports cards and memorabilia, but failed to ship any of the auctioned merchandise to the winning bidders. Bell argued that his conduct was "passive" and not deserving of the sentence enhancement. The court disagreed, however, and found that Bell's use of online auctions, which are available to millions of people, qualified as a "plan, program, promotion, or campaign" to defraud a large number of people under Sentencing Guideline § 2F1.1, which calls for a two-level enhancement in such circumstances.

Posting fraudulent advertisements for computer equipment on an Internet auction site (E-Bay) is "mass marketing" that qualifies a criminal defendant for a sentence boost under the federal Sentencing Guidelines, the U.S. Court of Appeals for the Tenth Circuit ruled April 5 in a decision designated as unpublished, United States v. Blanchett, 41 Fed. Appx. 181 (10th Cir. 2002).

D. Unlawful Internet Gambling Enforcement Act of "2006"

The Unlawful Internet Gambling Enforcement Act of 2006 was ushered through Congress by the Republican leadership in the final minutes before the election period recess. According to Sen. Frank R. Lautenberg (D-N.J.), no one on the Senate-House Conference Committee had even seen the final language of the bill. The Act is Title VIII of a completely unrelated bill, the Safe Port Act, HR 4954, dealing

with port security.

The new law was aimed at preventing Internet gambling by placing restrictions on the financial transactions that occur in connection with online wagering. The Act restricts electronic fund transfers and the use of credit cards in connection with such wagering. This means that players can no longer make wagers, or collect winnings using electronic fund transfers, credit or debit cards, or other online payment systems.

The Act requires the U.S. Treasury Department to issue regulations that would prohibit approving a transaction between a U.S.-based customer account and an Internet gambling merchant. Financial institutions would be required to follow those regulations, and would be subject to fines or penalties if they fail to comply.

The U.S. Justice Department has long taken the position that Internet gambling is illegal. The new law will add teeth to this position, and make it far more difficult for Internet gambling sites to obtain wagers from U.S. citizens.

The $12 billion Internet gambling industry is based outside the United States — most of the companies are British — though about half of its customers live in America. Lobbying for this bill were the horse racing industry and professional sports leagues, which argued that Web wagering could hurt the integrity of their sports. **The measure prohibits U.S. banks and credit card companies from processing payments to online gambling businesses outside the United States, took the British-based Internet gambling businesses by surprise** (??? Does not make sense as 1 sentence.). It prompted companies such as Sportingbet PLC and Leisure & Gaming PLC to sell their U.S. operations, and the industry lost an estimated 80% of its business as a result.

Half of the world's regular Internet gamblers live in the United States. United States gambling companies are barred by the terms of their gambling licenses to participate in Internet gambling. The law has been heavily criticized by the world trade community.

Early on, Citibank blocked customers from using its credit cards for online gambling transaction, under an agreement announced June 14, 2002, by then-New York Attorney General Eliot Spitzer (D).

According to Spitzer, other leading banks that have agreed to block online gambling transactions over the past several years are Bank of America, Fleet, Direct Merchants Bank, MBNA, and Chase Manhattan Bank.

In June 2009, the U.S. Department of Justice seized over $34 million belonging to over 27,000 accounts in the Southern District of New York Action Against Online Poker Players. This is the first time money was seized from individual players as compared to the gaming company. Jeff Ifrah, the lawyer for one of the account management companies affected, said that the government "has never seized an account that belongs to players who are engaged in what [Ifrah] would contend is a lawful act of playing peer-to-peer poker online."

Finally, June 1, 2010 the Act went into effect, exempting both lottery organizations as well as horse racing. The substantial delay between its passage and its enactment [some 5 years] caused its proponents heartburn in that it was widely believed that it allowed sufficient time for credit card processors to engineer ways around the law and for States such as New Hampshire to find a "work around" such as selling physical tickets to play online, thereby throwing them into the lottery ticket exception to its enforcement.

These fears were assuaged when the owners of the three largest online poker sites -- PokerStars, Full Tilt Poker and Absolute Poker -- were charged in the Southern District of New York in a Superseding Indictment handed down on April 15, 2011 with bank fraud, illegal gambling offenses and money laundering.

The Manhattan U.S. Attorney announced the indictments of those involved with the online poker sites as well as those who were responsible for the financial transactions, a total of eleven (11) defendants including both the ownership of the gambling sites as well as those responsible for the processing of credit cards.

Manhattan U.S. Attorney Preet Bharara said, "As charged, these defendants concocted an elaborate criminal fraud scheme, alternately tricking some U.S. banks and effectively bribing others to assure the continued flow of billions in illegal gambling profits".

As expected, the companies are all based overseas. The indictment sought $3 billion in money laundering penalties and forfeiture from the defendants.

The charges are conspiracy to violate Unlawful Internet Gambling Enforcement Act (UIGEA), violation of UIGEA, operation of illegal gambling business, conspiracy to commit

bank fraud and wire fraud, and money laundering conspiracy . Maximum penalties from these charges range from five years in prison and a $250,000 fine to 30 years in prison and a $1,000,000 fine (or twice the gross gain or loss).

Full Tilt Poker and PokerStars built lucrative businesses by catering to U.S. players from overseas. PokerStars is based in the Isle of Man, Full Tilt is regulated by Alderney in the U.K.'s Channel Islands and Absolute Poker, another site, is in Costa Rica.

The approach seemed to work, allowing the sites to build a market that last year included about 1.8 million people in the U.S. who played poker online for money, according to PokerScout, which tracks online poker site data. Other organizations say there are many more players.

The sites saw around $16 billion in wagers from U.S. players last year, with the bulk of that taken in by Full Tilt Poker and PokerStars, according to PokerScout.

The indictment and accompanying civil complaint alleged that the companies skirted the 2006 ban on electronic transfers related to gambling by working with third parties to create fictitious websites for fake companies to trick banks into thinking that it was not an Internet poker site. One was Green2YourGreen, an apparent environmentally-friendly household products company. In later years the sites invested in small U.S. banks in exchange for their cooperation in processing funds, the government alleges.

However, it should be noted that the ignominy of internet gambling apparently doesn't exist when the internet gambling involves a game that:

> "has an outcome that is determined predominantly by accumulated statistical results of sporting events…"

In other words: Fantasy Sports. So anyone interested in having a casino in their basement for fantasy sports betting can feel free to do so since the Act excludes them from its prohibition. Fanduel.com, Draftday.com, and Fanball.com are highly successful and fully operational.

---- ALERT ---- Shifting Sands?

On September 20, 2011, The Justice Department issued an opinion related to the attempts by both New York and Illinois to use the Internet and out-of-state transaction processors to sell lottery tickets to in-state adults.

The Justice Department is of the opinion that the use of these interstate transactions is not a violation of the Wire Act under Title 18 U.S.C. § 1084 (2006).

The D.O.J. limited its opinion to the lottery and, in fact, made it clear that the opinion had no bearing on any issue related to the Unlawful Internet Gambling Enforcement Act (U.I.G.E.A.). However, there are those that contend that the approval of across-state-line wire transactions for this one form of gambling puts the camel's nose under the tent toward the lifting of restrictions on other forms of online gambling.

The opinion can be found at:

http://www.justice.gov/olc/2011/state-lotteries-opinion.pdf

E. Internet Investment Scams

Internet investment scams continue to be on the increase. Federal prosecutors are actively investigating and prosecuting these cases.

Online schemes operating out of Nigeria that have defrauded victims out of tens of millions of dollars have become so pervasive that the U.S. Government began to exert its political muscle to inspire the West African country to take steps to decrease such crimes or face sanctions. These efforts may or may not be effective in reducing the fraud as such effects are essentially non-measurable.

Financial fraud is now reportedly one of the three largest industries in Nigeria, where the anonymity of the Internet is being used to give crime syndicates a windfall. One oft-used form of fraud is known as "419," a reference to Article 419 of the Nigerian criminal code, and involves scam artist sending an unsolicited e-mail, fax or letter proposing either an illegal or a legal business deal that requires the victim to pay an advance fee, transfer tax or performance bond or to allow credit to the sender of the message.

Victims who pay the fees are then informed that complications have arisen and are asked to send more payment, according to The 419 Coalition web site, which explains the scam.

The global scam, which has been going on since the early 1980s, had defrauded victims out of $5 billion as of 1996.

On June 28, 2001, the U.S. District Court for the Western District of Oklahoma issued a temporary restraining order and asset freeze against an alleged Internet investment swindler operating from British Columbia, Canada, and Lynden, Wash. (SEC v. Stroud, W.D. Okla., Case No. Civ-01-999 W, 6/28/01.)

The Securities and exchange Commission said it charged Stroud with conducting an Internet investment scheme involving investment-contract securities in which more than 2,200 investors worldwide have been fleeced of approximately $1 million.

In 2001, The Securities and Exchange Commission announced that Independent Financial Reports, Inc. was permanently enjoined in the U.S. District Court for the Central District of California from violating the anti-fraud provisions of the federal securities laws in connection with an alleged Internet stock manipulation scheme (Securities and Exchange Commission v. Sayre, C.D. Cal., Civil Action No. CV 00-03800 MMM (Ex) (5/31/01).

In its complaint, the SEC alleged that a tree trimmer masquerading as a financial analyst under the name IFR, publicly issued recommendations to buy shares in a publicly traded company, eConnect.

The complaint further charged that, prior to issuing the recommendations, Sayre bought several thousand shares of eConnect stock in accounts held by Silver Screen. After the IFR reports were widely disseminated on the Internet, Sayre allegedly took advantage of the market interest he had created by selling his eConnect stock into the inflated market

Tri-West Investment:

On December 20, 2004, Mr. Keith Nordick pled guilty to charges relating to the Tri-West Investment Club, an Internet-based investment fraud scheme that netted nearly $60 million. The Tri-West case is one of the largest Internet investment fraud cases in the country. Mr. Nordick pled guilty to one count of mail fraud, one count of wire fraud, and one count of conspiracy to commit money laundering. Nordick faces a maximum of 5 years in prison on each of the mail fraud and wire fraud charges and 20 years in prison on the money laundering charge, and faces fines of up to twice the value of the investors' losses. Sentencing was conducted by United States District Judge Edward J. Garcia and Nordick received 65 months in Federal Prison.

Tri-west was not a legitimate investment company and there never was any "Bank Debenture Trading Program." Instead, Tri-West was a vast "Ponzi" scheme that used more recent investor funds to make "dividend" payments to earlier investors to give the false impression of a successful investment program. None of the investors' money was invested as promised on the Web site, but instead was used to purchase millions of dollars worth of real property in Mexico and Costa Rica, as well as high-priced items such as a yacht, helicopter and numerous late-model cars. Millions of dollars were funneled to numerous bogus "shell" corporations that were created in Costa Rica for the purpose of concealing the ill-gotten gains. Tri-West duped approximately 15,000 investors to invest approximately $60 million for 1999 to September 2001.

F. New Anti-spam Legislation

On December 8, 2003, the House unanimously passed legislation that would, for the first time, establish national standards for sending unsolicited commercial e-mail messages.

The House approved a modified version of the CAN-SPAM Act (S. 877). The measure bans false or misleading unsolicited commercial e-mail, creates civil and criminal penalties for violators, and authorized the Federal Trade Commission to implement a "do-not-spam" registry.

The Senate approved its final version of the CAN-SPAM Act by unanimous consent November 25, 2003.

Under the legislation, which was signed by the President in December 2003, legitimate marketers could continue sending unsolicited commercial e-mail, as long as they follow certain rules, such as providing a mechanism for consumers to opt out of future messages.

"The CAN-SPAM bill will finally offer consumers the ability to put an end to the bothersome e-mail they see each day in their in-boxes," Senator Conrad Burns said in a statement.

The law required the FTC to report back to Congress within 24 months of the effectiveness of the act. No changes were recommended. It also

requires the FTC to promulgate rules to shield consumers from unwanted mobile service commercial messages. On December 20, 2005, a detailed report to Congress on the effectiveness of the Act indicated that the volume of spam has begun to level off, and due to enhanced anti-spam technologies, less is reaching consumer inboxes. A significant decrease in sexually explicit e-mail was also reported.

The CAN-SPAM Act is commonly referred to by anti-spam activists as the YOU-CAN-SPAM Act because the bill does not require e-mailers to obtain permission before they send marketing messages

Under the CAN-SPAM Act, violators can be imprisoned for five years and incur fines of up to $2 million, which can be tripled in cases of willful violations.

In January 2006, the first person charged under "CAN-SPAM", pled guilty to three felony counts in United States District Court in Ann Arbor, Michigan.

Daniel J. Lin, 30, of West Bloomfield, entered the guilty plea in United States District Court before Judge John Corbett O'Meara.

The information presented to the court at the time of the plea showed that between January 2004 and August 2004, Daniel Lin and others developed a business to marked and seel certain products, including weight loss patches, so called "generic" Viagra and Cialis pills, and other products through the use of "spam" or bulk commercial electronic mail. Lin caused hundreds of thousands of email messages advertising these products to be sent containing falsified header information, or by routing the messages through other computers without authorization. Mr. Lin was subsequently sentenced to a 36-month term of imprisonment.

On September 27, 2004, Nicholas Tombros plead guilty to charges and was one of the first spammers to be convicted under the Can-Spam Act of 2003. He was sentenced in July of 2007 to three years probation, six months house arrest, and fined $10,000.

On the horizon, however, is the implementation of Canada's Ani-Spam legislation which goes into effect in July 2014. It's said to be the one of the strictest and most aggressive anti-spam laws in the world. As their neighbors, our consumers should be

VIII. INTELLECTUAL PROPERTY CRIMES

The No Electronic Theft Act (NET Act) provides penalties for unlawful copying of copyrighted digital works.

The NET Act was enacted in order to close a loophole created by the ruling in the case United States v. La Macchia, 871 F. Supp. 535 (D. Mass. 1994).

La Macchia prevented the prosecution of a bulletin board operator who was providing users with free unauthorized copies of copyrighted software because the government was unable to prove that the operator benefitted financially from the copyright infringement.

The NET Act criminalized intentional acts of copyright infringement and removed commercial advantage or financial gain as a necessary element of the offenses.

There are four elements that need to be proved beyond a reasonable doubt to establish the felony offense of copyright infringement:

(1) a copyright exists;

(2) it was infringed by the defendant, specifically by reproduction or distribution;

(3) the defendant acted "willfully"; and

(4) the defendant infringed at least 10 copies of one or more copyrighted works with a total retail value of more than $2500 within a 180-day period.

See 17 U.S.C. § 506(a)(2); 18 U.S.C. § 2319(a), (c)(1). The Computer Crime and Intellectual Property Section of the Department of Justice has released a manual entitled: Prosecuting Intellectual Property Crimes, which goes into great detail regarding each of these elements. The manual is available online at www.cybercrime.gov/ipmanual.htm.

The first publicized judgment against an individual under the act was reported by the Justice Department in August 1999 when a University of Oregon student pleaded guilty to illegally posting software, musical recordings, and

digitally recorded movies on his Web site. Late in 1999, the U.S. Sentencing Commission finally proposed new sentencing guidelines under the act. U.S.S.G. § 2B5.3.

Two participants in one of the world's most sophisticated Internet piracy schemes agreed January 22, 2002, to plead guilty to charges of criminal copyright infringement, in the first criminal case brought as a result of the U.S. department of Justice's "Operation Buccaneer." United States v. Nguyen, C.D. Cal., No. CR 02-63, January 22, 2002. They were members of an Internet piracy or "Warez" group known as DrinkorDie, which contained thousands of pirated software titles, including Windows operating systems, video games, and DVD movies. DrinkorDie was the Warez group targeted by Operation Buccaneer, in which 58 search warrants were simultaneously executed December 11, 2001, in the United States, Australia, Finland, England, and Norway (see *ccLR* vol. 1, no. 18, December 17, 2001). The searches led to the seizure of more than 100 computers.

The U.S. District Court for the Northern District of Illinois ruled on June 14, 2002, that the mere fact that no previous defendants convicted under the No Electronic Theft Act had been sentenced to imprisonment did not mean that imprisonment was inappropriate for an NET Act violator.(United States v. Rothberg, 222 F. Supp. 2d 1009 (N.D. Ill. 2002) The court pointed to the defendant's failure to make an adequate showing that his case was similar to the previous cases in which defendants were given probation.

Robin Rothberg was one of 17 defendants charged in connection with the prosecution of the Pirates With Attitudes, a web-based network that allegedly made $1.4 million worth of computer software available to paying members to make unauthorized copies.

Rothberg pleaded guilty to conspiracy under 18 U.S.C. § 371 to commit copyright infringement in violation of 17 U.S.C. § 506(a)(2) and 18 U.S.C. § 2319(c)(1). He was sentenced to 24 to 30 months in prison.

On September 8, 2006, in *U.S.A. v. Peterson*, the Defendant was sentenced in the Eastern District of Virginia to 87 months in federal Prison for operating the http://www.ibackups.net Web site which sold copies of software products that were copyrighted by companies such as Adobe Systems Inc., Macromedia Inc., Microsoft Corporation, Sonic Solutions and Symantec Corporation at prices substantially below the suggested retail price. The software products purchased on Peterson's Web site were reproduced and distributed either by instantaneous computer download of an electronic copy and/or by shipment through the mail on CDs. Peterson often included a serial number that allowed the purchaser to activate and use the product.

Additional DOJ piracy prosecutions include:

- On June 28, 2006, 2 individuals were convicted as a result of operation FastLink. These are the first federal criminal sentences for members of the so-called "warez scene" from the Charlotte component of Operation FastLink, an ongoing federal crackdown against the organized piracy groups responsible for most of the initial illegal distribution of copyrighted movies, software, games and music on the Internet. Operation FastLink has resulted, to date, in more than 120 search warrants executed in 12 countries; the confiscation of hundreds of computers and illegal online distribution hubs; and the removal of more than $50 million worth of illegally-copied copyrighted software, games, movies and music from illicit distribution channels.
- "Operation Decrypt," which yielded the Feb. 11, 2003, indictment of 17 individuals for their roles in developing sophisticated software for stealing satellite TV signals;
- In September, 2004, Operation Gridlock was the first federal enforcement action taken against criminal copyright piracy on peer-to-peer networks. Federal agents executed six search warrants at five residences and one Internet service provider in Texas, New York, and Wisconsin, as part of an investigation into the illegal distribution of copyrighted movies, software, games, and

music over peer-to-peer networks. Agents seized computers, software, and computer-related equipment in the searches.

IX. THE PRIVACY PROTECTION ACT OF 1980, 42 U.S.C. § 2000AA

The Privacy Protection Act of 1980 (PPA) was enacted by the United States Congress in response to the decision in Zurcher v. Stanford Daily, 436 U.S. 547 (1978).

Although the PPA was originally designated to protect traditional publishers such as the media and authors of articles and books, it has already made its impact felt in the computer crime investigations. See e.g.,Steve Jackson Games, Inc. v. United States Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993), *aff'd.* Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457 (5th Cir. 1994). There are four exceptions to the general prohibition against using warrants to obtain documentary materials. These exceptions are set forth in 42 U.S.C. § 2000aa(b) and include:

(1) Probable cause to believe that the "person possessing such materials has committed or is committing the criminal offense to which the materials relate;"

(2) Reason to believe that immediate seizure of the work product materials is necessary to prevent the death or serious bodily injury of a human being;

(3) Reason to believe that giving notice pursuant to a subpoena duces tecum would result in destruction, alteration, or concealment or such materials; or

(4) Such materials have not been produced in response to a court order directing compliance with a subpoenas duces tecum and (A) all appellate remedies have been exhausted; or (B) there is reason to believe that the delay in an investigation or trial would threaten the interests of justice.

In summary, the PPA requires law enforcement officers – absent exigent circumstances – to rely on subpoenas (as opposed to search warrants) to acquire materials which are reasonably believed to be intended for publication unless there is probable cause to believe that the person possessing the material has committed or is committing a crime. Under the PPA, a civil cause of action for monetary damages may be brought against the law enforcement agency and potentially, against the individual officers in their personal capacity, should they conduct a search or seizure of materials in violation of this Act.

However, on July 2, 2001, the U.S. Court of Appeals for the Sixth Circuit held that the Privacy Protection Act of 1980 does not prevent law enforcement officials from seizing data otherwise protected under the act if those materials are commingled with evidence of crime on a suspect's computer. Guest v. Leis, 255 F.3d 325 (6th Cir. 2001).

The court expressed disagreement with Steve Jackson Games v. U.S. Secret Service, 816 F.Supp. 432 (W.D. Tex. 1993), affd Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457 (5th Cir. 1994) which held that authorities must notify users of a bulletin board prior to searching even when proceeding under valid search warrant.

The previous version of the statute required police to obtain a subpoena prior to searching or seizing work product or other materials reasonably believed to pertain to public communications. Congress amended the statute in 1996 to ensure that it does not protect persons disseminating child pornography. Although the previous version of the statute arguably excluded the dissemination of child pornography, the revised statute explicitly precludes such an exception. Section 2000aa now permits officers to search and seize computer equipment and files intended for public dissemination upon probable cause that the offense "involves the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography."

X. PORNOGRAPHY AND THE INTERNET

Prior to the Internet, pornography was usually produced and distributed in the form of photographs and magazines. The photographs and film were commercially processed. Distribution was accomplished by the mail or the use of clandestine distribution networks. With the development of video technology, commercial film production was no longer necessary. Hand-held camcorders allowed individuals to produce pornography videos at any location.

This decade has seen the emergence of a new medium for pornography: the Internet. The result has been a tremendous expansion of the pornography industry. Child pornography was significantly curtailed in the United States in the 1980s. There has been a resurgence that started in the 1990s due to unregulated news groups, chat rooms, and commercial on-line services.

There are numerous reasons for the profusion of pornography on the Internet and computer bulletin boards. If one has access to a computer and a modem, one has access to pornography. Photographic images from pictures or books can be input into a computer using scanners, devices that convert images into digital form that may be saved as files on a hard disk. Computer technology has revolutionized the distribution of pornography. Material can now be exchanged on small floppy disks or by way of the Internet rather than through the mail or personal contact. Furthermore, users and distributors are provided with substantial anonymity on the Internet.

It has been reported that the United States is the largest consumer market in the world for child pornography.

A. Law Enforcement Operations

1. Historical Perspective

While investigating the disappearance of a juvenile in 1993, FBI agents identified two suspects who had sexually exploited numerous juvenile males over a 25 year period. Investigation into the activities of the suspects determined that adults were routinely utilizing computers to transmit images of minors showing frontal nudity or sexually explicit conduct. Further FBI investigation revealed that the utilization of computer telecommunications was rapidly becoming one of the most prevalent techniques by which some sex offenders shared pornographic images. Based on information developed during this investigation, the Innocent Images National Initiative created in 1995 to address the illicit activities conducted by users of commercial and private online services as well as the Internet.

In 2000, the Crimes Against Children program was formed from the Violent Crimes Section of the FBI's Criminal Investigative Division. It was under this umbrella that programs such as the Innocence Lost National Initiative and Child Abduction Rapid Deployment Teams were then implemented to provide additional resources and response tools to combat the ever-present problems of child prostitution, child abduction, and child sex tourism.

In October 2012, the Crimes Against Children program and the Innocent Images National Initiative merged to form the Violent Crimes Against Children program in the Criminal Investigative Division. The program now continues the efforts of both former iterations, providing centralized coordination and analysis of case information that is national and international in scope, requiring close cooperation not only among FBI field offices and legal attachés but also with state, local, and international governments.

This is merely an example of the FBI response and is consistent with coordinated efforts under Homeland Security, which uses Operation Predator to brings together an array of resources to target these child predators. As part of the effort, CSI participates on all 61 Internet Crimes Against Children (IAC) Task Forces across the United States, which are led by state and local law enforcement agencies. They established a National Victim Identification Program at its Cyber Crimes Center, combining the latest technology with traditional investigative techniques to rescue child victims of sexual exploitation.

CSI is also the U.S. representative to the Interpol working group that locates new child sexual abuse material on the Internet and refers cases to the country that the abuse is believed to be occurring in for further investigation. Also, CSI special agents stationed internationally work with foreign governments, Interpol and others to enhance coordination and cooperation on crimes

that cross borders.

CSI has stepped up its efforts works by partnering with the National Center for Missing & Exploited Children and other federal agencies to help solve cases and rescue sexually exploited children.

From a law enforcement perspective, child exploitation offenses have been frown in priority since the first investigation by a U.S. agency was undertaken that targeted the use of computers to traffic in child pornography. This was done by the U.S. Customs Service (USCS) in 1992.

2. Noteworthy Operations

On May 20, 2014, more than 70 people, including a police officer, a Boy Scout leader, a Little League Coach, and a rabbi, were all arrested in one of the largest ever New York City round-ups of suspected child pornography possessors, distributors, and producers. The investigation took only five (5) weeks and centered around peer-to-peer networks consisting of more than6700 computers and 175 terabytes of data.

On August 8, 2001, DOJ announced that Operation Avalanche, a coordinated strike by the U.S. Postal Service and 30 federal Internet Crimes Against Children Task Forces, has resulted in 144 searches and 100 arrests on charges of trafficking child porn through the mail and the Internet. Five international webmasters from Russia and Indonesia have also been charged but remain at large.

The investigation began in 1999 with a Fort Worth, Texas, company called Landslide Productions, Inc., operated and owned by Thomas Reedy, 37, and his wife Janice, 32. Postal inspectors found that the Landslide website, which had a t least 250,000 subscribers, admitted customers into Web pages containing graphic pictures and videos of children engaged in sexual acts.

In one month alone, the business grossed as much as $1.4 million, most of it from child porn, officials said.

The couple were convicted. Thomas Reedy was sentenced to 1,335 years in prison and his wife to 14 years. This was the first life sentence in federal court for child pornography.

U.S. Customs announced August 10, 2002, a joint European-U.S. investigation of an international pedophile ring that included parents who allegedly sexually abused their own children and distributed images of children as young as 2 years old over the Internet. The investigation was called Operation Hamlet, a 10-month probe that included the Customs Service, Danish national police, the Justice Department and the U.S. attorney's offices around the United States. The ring allegedly abused and exploited at least 45 children, 37 of whom are citizens and residents of the Untied States, officials said. The ages of the 37 children range from 2 to 14.

Fifteen members of the ring were charged in an indictment in U.S. District court in the Eastern District of California. According to the indictment, all 15 were charged with conspiracy, two with sexual exploitation and one with receiving and distributing materials involving sexual exploitation of minors. Nine of the people were Americans and the other six were Europeans. The investigation is continuing. The 15 are from California, Texas, Idaho, Florida, Washington state, South Carolina, Kansas, Denmark, Switzerland, and the Netherlands, according to the indictment.

On March 19, 2002, the FBI announced that 27 people who had confessed to molesting 36 children had been arrested in a major investigation into child pornography over the Internet. The 14 month investigation of the international ring involved all 56 FBI field offices across the U.S. The investigation, dubbed "Operation Candyman," focused on an e-group, or online "community," whose 7,000 members uploaded, downloaded or traded images of sexually exploited children. Ninety individuals in 20 states were arrested. The included members of the clergy, law enforcement officers, a nurse, a teacher's aide, and a school bus driver. Investigators identified 7,000 e-mail addresses linked to the "candyman" e-group, with 4,600 in the United States and 2,400 in other countries.

On September 3, 2003, an Internet site owner was arrested on charges that he created and used misleading domain names on the Web to deceive minors into logging on to pornographic sites. John Zuccarini, 53, was arrested on September 3, 2003, in a Florida hotel room. The prosecution is the first of its kind to be brought under the Truth in Domain Names Act, enacted as part of the "Amber alert" legislation, making it a crime to entice children to Internet porn. Prosecutors say Zuccarini is accused of registering at least 3,000 domain names and earing up to $1 million per year from them.

Zuccarini registered various domain

names that consisted of misspellings of legitimate domain names that are popular with children – including Bob the Builder, Britney Spears, NSync, DisneyLand, and the Teletubbies. For example, he registered www.dinseyland.com instead of www.disneyland.com. Upon accessing Zuccarini's sites, the viewer would be directed to Web pages depicting graphic sex and advertising additional online porn.

Endangered Child Alert Program

On February 21, 2004, the FBI began its Endangered Child Alert Program (ECTP) as a new proactive approach to identifying unknown individuals involved in the sexual abuse of children and the production of child pornography. A collaborative effort between the FBI and the National Center for Missing & Exploited Children, ECTP seeks national and international exposure of unknown adults (referred to as John/Jane Does) whose faces and/or distinguishing characteristics are visible in child pornography images. These faces and/or distinguishing marks (i.e. scars, moles, tattoos, etc.) are displayed on the Seeking Information section of the FBI website as well as various other media outlets in hopes that someone from the public can identify them.

As a result of ECTP, the faces of many Jane/John Does have been broadcast on television shows such as America's Most Wanted: America Fights Back, The Opah Winfrey Show, and The O'Reilly Factor.

Operation Rescue Me

On June 24, 2008, the FBI—in partnership with the National Center for Missing & Exploited Children—began Operation Rescue Me, an aggressive program that uses image analysis to determine the identity of child victims depicted in child sexual exploitation material.

Focusing on items seen in the backgrounds of child pornography images and videos, analysts attempt to identify and subsequently rescue victimized children.

3. First Conviction Under Section 2251A of the Protect Act Since the Enhanced Penalties Became Effective

In April 2006, U.S. District judge Richard D. Bennett, District of Maryland, sentenced Thomas C. Moser, age 37, of Leighton, Pennsylvania, to 30 years in prison, followed by supervised release for life. In addition, Judge Bennett ordered that Moser must register as a sex offender for the remainder of his life, have no unsupervised contact with minors, and cannot use a computer without prior approval of the U.S. Probation Office.

Moser was convicted on January 9, 2006 of using the internet to entice a minor to engage in sexual activity, interstate travel to engage in a sexual act with a minor and using the internet to obtain control of a minor for the purpose of producing child pornography.

According to testimony presented at trial, in May 2005 Moser contacted an undercover postal inspector in an internet chat room partially entitled "incest." Moser continued his on-line conversations with the postal inspector and asked if he could travel from his home in Pennsylvania to Frederick, Maryland in order to have sexual relations with the undercover postal inspectors 14 and 12 year-old daughters. Moser also stated he would bring photographic equipment with him to record his sexual activities with the girls.

The postal inspector testified that he and Moser agreed to meet on September 9, 2005 at a store in Frederick, Maryland. After confirming by telephone that he was on his way, Moser arrived in Frederick, Maryland at the agreed upon time and was arrested by federal agents and detectives from the Frederick County Sheriff's Office.

This is believed to the first conviction under Section 2251A of the Protect Act enacted on April 30, 2003, which prohibits a person having custody or control of a minor from offering to obtain control of a minor for the purpose of producing child pornography. Section 2251A imposes a mandatory minimum sentence of 30 years in prison.

4. Internet Providers to Create Database to Combat Child Pornography

On July 11, 2006, it was announced that five leading online service providers will jointly build a database of child-pornography images and develop other tools to help network operators and law enforcement better prevent distribution of the images.

The companies pledged $1 million dollars

among them Tuesday to set up a technology coalition as part of the National Center for Missing and Exploited Children. They aim to create the database by year's end, though many details remain unsettled.

The participating companies are Time Warner Inc.'s, Yahoo Inc., Microsoft Corp., EarthLink Inc. and United Online Inc., the company behind NetZero and Juno.

The announcement came as the U.S. government began pressuring service providers to do more to help combat child pornography. Top law enforcement officials have told Internet companies they must retain customer records longer to help in such cases and have suggested seeking legislation to require it.

AOL chief counsel John Ryan said the coalition was partly a response to a speech in April of 2006 by then-Attorney General Alberto R. Gonzales during which he identified increases in child-porn cases and chiding the Internet industry for not doing more about them.

AOL, for instance, planned to begin checking e-mail attachments that are already being scanned for viruses. If child porn is detected, AOL would refer the case to the missing-children's center for further investigation, as service providers are required to do under federal law.

The companies involved said they are talking with other service providers about joining. But companies that do not participate still are required by law to report any suspected child-porn images, and many already have their own techniques for monitoring and identifying them.

B. Computer Bulletin Boards, Definitions and Graphics Technology

1. Computer Bulletin Boards and Electronic Mail

A BBS is a simple operation: essentially, it is a computer which allows other computers to connect with it. The BBS receives messages from other computers and allows users to read the messages. The number of users connecting to a BBS can range from a few to thousands. This simple operation allows for quick and expansive communication.

Although the BBS networks provide expansive communication, a BBS is only one part of the vast communication network available through online services. The parent of the BBS networks is the Internet. The Internet links thousands of BBS networks. The BBS, in turn, is the subsection of the online service, which allows communication through a public forum.

In addition to bulletin boards, an online service provides other services which enable users to communicate. For instance, an online service might offer electronic mail. E-mail messages provide greater privacy than the posting of messages on BBS networks because a user can send e-mail directly to a party.

E-mail is the most private form of electronic communication because users can secure their e-mail with passwords. However, an outsider may still discover the password and thus, view the e-mail. In order to increase the privacy of e-mail messages, BBS networks and the Internet recently developed a system of public-key encryption.

Public-key encryption is the encoding of messages. One system of encryption is called Privacy Enhanced Mail (PEM). With PEM, a user has a public key and a private key. A user can send messages to another user by placing the recipient's public key number on the message. In order to view the message, the user must decrypt or decode the message with the private key number. The private key is the only way to access the message. Accordingly, this technology provides greater privacy for e-mail messages.

2. Child Pornography Definition

Prior to September 30, 1996, in any federal child pornography case, the government had to prove beyond a reasonable doubt that the images involved actual minors. 18 U.S.C. §§ 2252, 2256(1) (1996) (defining "minor" as any person under the age of 18 years). Currently, Child Pornography is defined as any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, involving a minor. As of April 19, 2003, Newly amended 18 U.S.C. § 2256(8) defines "child pornography" to also include computer or digital visual depictions that are **indistinguishable** from pictures of actual minors. "Indistinguishable" means that an "ordinary

person viewing the depiction would conclude that the depiction is of an actual minor." Note that drawings, cartoons, sculptures or paintings are specifically excluded. Section 2256(11). It was Congress' express intent to include within the definition of "child pornography" images that never involved actual minors. The images could involve adults depicted as minors or images created wholly from a computer program. *See generally* S. Rep. 358, 104th Cong., 2d Sess. (1996) (available on Westlaw as 1996 WL 506545 (Leg. Hist.)).

After, the U.S. Supreme Court struck down the portions of the CPPA that criminalized the possession of distribution of "virtual child pornography." Ashcroft v. Free Speech Coalition, 122 S.Ct. 1389 (2002), the 2003 "legislative fix" was to delete the phase "appears to be", and substitute in the word "indistinguishable".

"Virtual Child Pornography"

In "virtual child pornography," no sexual conduct by children is occurring, as the images reflect either a completely imaginary child, or a real child, but one who has not engaged in any sexual conduct. Thus, the images are "virtual" as opposed to "real" pornography. The images only appear to represent real children.

Virtual child pornography can be created by putting an innocent picture of a real child through a scanner, and converting it into an image which can then be manipulated into pornography. A pornographer can create virtual child pornography by using various computer graphics programs to create the picture of an imaginary child. For example, a pedophile would obtain an innocent picture of a real child, such as those found in department store catalogs. He would then use a scanner to turn this picture into a computer file. At that point, he can bring the image up on his computer screen using a graphics viewer, and he can edit the picture however he chooses using graphics software. He could insert the child's face into pornographic pictures of adults that he has obtained from legal magazines and scanned into his system. With a little editing, he can make it appear as though the child is engaging in any sort of sexual activity.

A section 2251(a) exploitation of a male was not made because defendant never engaged in any actual or simulated sexually explicit conduct, but rather only "[a] picture of his face was taken and later – without his knowledge or consent – superimposed on a picture exhibiting the genitals of one not shown to be a minor. United States v. Carroll, 190 F.3d 298 (5th Cir. 1999). Defendant's action in superimposing a photograph of the face of an identifiable minor on an image of a nude body is not conduct proscribed by 18 U.S.C. § 2251(a). United States v. Reinhart, 227 F.3d 651 (5th Cir. 2000) (en banc).

"Pseudo Child Pornography"

The term "pseudo-child pornography" refers to pictures, in which young-looking actors who have reached the age of majority play the parts of young children. The performers only appear to be below the legal age. As stated above, the term "virtual child pornography" refers to pornographic images which have been produced with the use of a computer graphics program, and in which no real child was sexually abused or exploited in the making of the image. The computer equipment and expertise required to produce high-tech pornography is readily available to any individual. All a pornographer needs is a personal computer with a few inexpensive and easy-to-use accessories, such as a scanner, image editing and morphing software costing as little as $50 to $100, all available at virtually any computer store or through mail order computer catalogs.

A scanner is a computer device which converts hard copies of pictures into binary computer files, which can then be stored on the computer hard drive just as any other file.

C. The Relevant Statutes

1. Protection of Children From Sexual Predators Act of 1998

On October 30, 1998, President Clinton signed Public Law 105-314 into existence. This Act known as the "Protection of Children From Sexual Predators Act of 1998" made several significant changes to both of these statutes and in some cases double the maximum terms of confinement. The most important change was the amendment of both 18 U.S.C. § 2252 and 18 U.S.C. § 2252A to reflect a "zero tolerance" for those possessing child pornography. Under these amendments, the government now must only show that the subject possessed one or more images

containing child pornography. (Until this change, the government was required to prove that the subject possessed three or more images.) The amendment also creates an affirmative defense for the possession of child pornography, which were added as subsection (c) to 18 U.S.C. § 2252 and as subsection (d) of 18 U.S.C. § 2252A, respectively. While there are some differences in the wording of these two subsections, generally they provide that it shall be an affirmative defense to a charge of violating these acts if the subject – (1) possessed less than three images of child pornography; and (2) promptly and in good faith, and without retaining or allowing any person, other than a law enforcement agency, to access any image or copy thereof – (A) took reasonable steps to destroy such image; or (B) reported the matter to a law enforcement agency and afforded that agency access to each such image.

As a result of the ruling in Ashcroft v. Free Speech Coalition, 122 S.Ct. 1389 (2002), however, federal prosecution are limited to pornography involving real children under the 1988 Act.

2. The Previous Version: 18 U.S.C. 2252A

The Child Pornography Prevention Act of 1996, which became effective on September 30, 1996, was enacted in large part to remedy a loophole in the earlier version regarding the illegality of computer-generated or morphed child porn, even where no actual children have been used to produce the images.

Among other things, the statute punishes the knowing transmission, receipt, or distribution of child pornography in interstate or foreign commerce. § 2252A(a)(1)-(2). It also more broadly punishes the knowing possession of any material containing three or more images of child pornography, provided the requisite interstate or foreign nexus is established. § 2252A(a)(4)(B).

Written into the statute is an affirmative defense for material produced using actual adults, rather than minors, and which was not marketed as child pornography. § 2252A(c).

The statute retains the old definition of sexually explicit conduct: "actual or simulated (A) sexual intercourse...; (B) bestiality; (c) masturbation; (D) sadistic or masochistic abuse; or (E) lascivious exhibition of the genitals or pubic area of any person." § 2256(2).

Note that for purposes of the statute, a minor is someone under 18 years of age. § 2256(1).

3. The Earlier Version: 18 U.S.C. § 2252

This earlier version of the statute remains in effect, although its continued vitality is questionable.

The prohibited offenses are analogous to § 2252A, although its scope is narrower due to its more restricted definition of objectionable depictions. For example, under the old statute, it was possible to argue that the transmission, receipt, or possession of morphed depictions of child pornography was not illegal and that the government had to prove that the depictions were of actual minors. See United States v. Lamb, 945 F. Supp. 441, 454 (N.D.N.Y. 1996).

The old statute also narrowly limited prosecutions for possession of child porn. Under its formulation, a person could be convicted for possession of child porn only if he possesses three or more matters containing visual depictions of child pornography (*e.g.,* three or more pornographic books or magazines). § 2252(a)(4)(B). Under the 1996 statute, a person can be convicted for possessing just one matter if it contains three or more images of child pornography (*e.g.,* just one book with multiple pictures). § 2252A(a)(4)(B).

4. The 2003 PROTECT Act.

The 2003 Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act (The PROTECT Act) was passed by Congress on April 9, 2003. It was signed by President Bush on April 30, 2003, which is the effective date of the PROTECT Act.

The 2003 Act contains many important provisions amending 2252 and 2252A. Major revisions include:

-New Statute of Limitations for Child Abduction (+) Sex Crimes.

-New Pandering Provision.

-New Expanded Pornography Definition.

(The legislative fix to the Free Speech case)

-New Obscenity Provision (§1466A)
-New Sentencing Provisions
-Expansion of Sex Tourism Statutes
-New International Parental Kidnaping Statute.
-Amber Alert Provisions

Mandatory Minimums: The 2003 Amendments to both 18 U.S.C. §§ 2252 and 2252A increased the mandatory minimums and statutory maximums.

Possession of Child Pornography:

- 1st Offense: new max is 10 years (was 5)
- 2nd Offense: new max is 20 years (was 10)
- **new mandatory minimum is 10 years** (was 2)

Receipt, Transmission, Distribution, Sale, Etc.:

- 1st Offense: new max is 20 years (was 15)
- **new mandatory minimum is 5 years**
- 2nd offense: new max is 40 years (was 30)
- **new mandatory minimum is 15 years**

5. Child Protection Act of 2012

On December 7, 2012, the President signed the Child Protection Act of 2012 into law. The Act advanced several initiatives including:

- The federal criminal code would be amended to increase the prison term from 10 to 20 years for possession etc. of child pornography depicting children 12 years of age and younger.
- A U.S. district court would be required to issue a protective order on their own motion under certain circumstances that would prohibit harassment or intimidation of a minor victim or witness.
- Funds for the national Internet Crimes Against Children Task Force would be re-authorized, with the Attorney General being given authority to actually double training funds for task force members and other executive and judicial officials.
- The Attorney General would be required to appoint a senior official at the Dept. of Justice to be the National Coordinator for Child Exploitation Prevention and Interdiction, who would be responsible for coordinating the National Strategy for Child Exploitation Prevention and Interdiction.
- The U.S. Marshals would be authorized to issue administrative subpoenas in their investigations of unregistered sex offenders.

6. Other Related Statutes

The production of child pornography is punishable under 18 U.S.C. § 2251, while the buying or selling of children for purposes of producing child porn is prohibited under 18 U.S.C. § 2251A.

Sexual abuse crimes involving children may be punishable under 18 U.S.C. § 2241-2248 and 18 U.S.C. § 2421-2423.

See United States v. Somner, 127 F.3d.405 (5th Cir. 1997), regarding the interstate transportation of a minor with the intent to engage in illegal sexual activities with the minor; 18 U.S.C. § 2423(a).

Sending death threats over the Internet is a possible violation of 18 U.S.C. 875(c).

Texas Penal Code § 43.26; Possession or Promotion of Child Pornography. Texas Penal Code § 43.25(f); Affirmative Defenses

7. Definitions, Elements and Jury Instructions, and Duplicative Charging

Visual Depictions

Computer GIF files (*i.e.* graphic interchange format files used to store information like photographs) constitute visual depictions under the pre-1996 version of the statute. United States v. Hockings, 129 F.3d 1069, 1071-72 (9th

Cir. 1997). Note that the new statute explicitly provides that a "visual depiction" includes "data stored on computer disk or by electronic means," § 2256(5), and that now, a person can be convicted for possession of merely three or more images (*i.e.,* no more need to prove possession of three of more matters containing images).

Under § 2252, "a cartoon character, a computer-animated image, a person eighteen or over who appears to be a minor, or an image of... an adult 'doctored' by computer or other means to appear younger are not covered." United States v. Lamb, 945 F. Supp. 441 (N.D.N.Y. 1996).

Mens Rea and Knowledge

In United States v. Crow, 164 F.3d 229 (5th Cir. 1999), the defendant contended that the Court's instructions on the scienter and *mens rea* elements of § 2251(a) and (d) were inadequate and resulted in plain error. The defendant asserted that the government was required to show that he actually "knew" that _____ was a minor, rather than instructing the jury that it was permitted to convict if they found the defendant simply "believed" that _____ was a minor.

In disagreeing with the defendant's position, the Fifth Circuit relied on United States v. United States District Court for the Central District of California, 858 F.2d 534, 538 (9th Cir. 1998), wherein the Ninth Circuit held that under § 2251(a), "a defendant's awareness of the subject's minority is not an element of the offense."

Also see United States v. Griffith, 284 F.3d 338 (2nd Cir. 2002). For prosecutions under sections 2251(a) or 2423(a), government is not required to prove that defendant knew victim's age.

Crow also contended that the district court plainly erred in failing to properly and adequately instruct the jury on the scienter element in count five in violation of his Fifth and Six Amendment rights. Count five alleged a violation of 18 U.S.C. § 2252(a)(2), which makes it a crime to knowingly receive any visual depiction of a minor engaged in sexually explicit conduct via interstate commerce. Crow asserted that the court failed to instruct the jury that he must have known that the individual depicted was a minor as shown in United States v. X-Citement Video, Inc., 513 U.S. 64 (1994). The Court did not find plain error in the court's instructions to the jury.

In order to convict a defendant under § 2252, the government must prove that the defendant knew of the sexually explicit nature of the images and of the minority of the performers. United States v. X-Citement Video, Inc., 513 U.S. 64 (1994).

A defendant may be convicted of unlawful possession of child pornography under § 2252(a)(4)(B) "only upon a showing that he knew the matter in question contained an unlawful visual depiction." United States v. Lacy, 119 F.3d 742, 747 (9th Cir. 1997) .

United States v. Tucker, 305 F.3d 1193 (10th Cir. 2002). Defendant claimed that he did not knowingly possess child pornography images that were found in his cache file, because he only meant to view the images on the internet and not to possess them. Court rejected this argument and found that defendant's knowledge of the existence of the cache file was sufficient to show knowing possession of the images located there.

Matters and Materials

Defendant Charles Dauray was arrested in possession of pictures (or photocopies of pictures) cut from one or more magazines. He was convicted following a jury trial of violating 18 U.S.C. § 2252(a)(4)(B), which punishes the possession of (*inter alia)* "matter," three or more in number, "which contain any visual depiction" of minors engaging in sexually explicit conduct. On appeal from the judgment of conviction, Dauray argued that the wording of § 2252(a)(4)(B) – which has since been amended – is ambiguous as applied to possession of three or more pictures, and that the rule of lenity should therefore apply to resolve this ambiguity in his favor. The court reversed the conviction, and directed that the indictment be dismissed. United States v. Charles R. Dauray, 215 F.3d 257 (2d Cir. 2000).

Contrary to the government's contention that a computer GIF file containing a visual depiction is a "matter" under the statute, the court held that the relevant "matter" is "the physical medium that contains the visual depiction" (*i.e.,* the computer disks and hard drive). Lacy, 119 F.3d at 748, *cf.*, United States v. Hall, 142 F.3d 988-99 (7th Cir. 1998).

"Materials" mean not only tangible matters that go into a visual depiction (that

become an ingredient of the depiction) but also tangible matters that are use to give being, form or shape to, but do not necessarily become a part of ingredient of the visual depiction, such as computers or floppy disks; with respect to the jurisdictional nexus, the question is were the visual depictions contained on the diskettes produced using materials that traveled in interstate commerce? Although the diskettes themselves traveled in interstate commerce, there was a lack of proof that the diskettes were actually used to produce the graphic files; it was unclear from the testimony at trial whether a computer graphics file is produced or created prior to being recorded on a storage media but instead comes into being at or after being recorded, and as a result, the proof failed. (Conviction reversed, acquittal entered.) United States v. Wilson,182 F.3d 737 (10th Cir. 1999).

Interstate Commerce

The required jurisdictional element is established "if the 'pictures or the materials used to produce them' traveled in interstate commerce.'" In this case, under the "materials" prong, the government must prove that the computer hard drive and disks themselves had traveled in interstate commerce, rather than that the computer's components so traveled. Lacy, 119 F.3d at 749.

The interstate commerce element of § 2252(a)(2) is satisfied if the child pornography was *ever* shipped or transported in interstate commerce. In addition, the electronic transmission of information across state lines or *across the street* over the Internet or an on-line computer service occurs in interstate commerce (*i.e.,* transmission in "cyberspace" is transportation in interstate commerce). United States v. Smith, 47 M.J. 588 (Navy-Marine Ct. Crim. App. 1997); see also United States v. Carroll, 105 F.3d 740 (1st Cir.), and United States v. Runyan, 290 F.3d 233, 239 (5th Cir. 2002). Possession of child pornography photographs taken solely within one state, but with the use of film manufactured in another state, involves a sufficient interstate nexus. United States v. Winningham, 953 F. Supp. 1068 (D. Minn. 1996). See also United States v. Kallestad, 236 F.3d 225 (5th Cir. 2000).

Evidence that defendant's computer was connected to Internet and contained child pornography on its hard drive, and that defendant had viewed pornographic images on Internet was insufficient to sustain conviction for possession of three or more matters containing visual depictions of minors engaged in sexually explicit conduct, which were produced using materials shipped or transported in interstate commerce. This is true even if one image from the hard drive had a website address embedded on it and witness testified that defendant had viewed another image on the Internet, absent evidence connecting the third image to the Internet. 18 U.S.C. § 2252A(a)(5)(B). United States v. Henriques, 234 F.3d 263 (5th Cir. 2000). Note: the statue at issue in Henriques required the possession of at least 3 images of child pornography.

In United States v. Mohrbacher, 182 F.3d 1041 (9th Cir. 1999), the government charge defendant with receiving and possessing child pornography, as well as transportation because Mr. Mohrbacher downloaded child pornography from a foreign-based electronic board. He admitted to receiving the images in violation of § 2252(a)(2) but denies transporting or shipping them in violation of § 2252(a)(1). The court agreed and said the government overcharged. U.S. v. Colavito, 19 F.3d 69 (2d Cir. 1994). Receipt and possession case. Section 2252(a)(4)(B) "lists several means by which pornography may travel between states, including the transmission of visual images across telephone lines by way of computer modems." The defendant must know that he is receiving material through interstate commerce and the materials contain sexually explicit depictions of minors.

United States v. Simpson, 152 F.3d 1241 (10th Cir. 1998), also discusses on the interstate commerce issue. Simpson is especially interesting, given the depth of the Court's discussion of the inner workings of a computer and how files stored on a computer can be traced to Internet downloading sessions.

The limits of Congress' authority under the interstate commerce clause of the Constitution was the focus in United States v. Bausch, 140 F.3d 739 (8th Cir. 1998). Bausch had taken several pictures of two girls, aged fifteen and sixteen, while they were nude. These photos showed the girl's exposed genitalia and depicted the girls engaging in sexually suggestive conduct to include simulated oral sex. After conviction, Bausch appealed arguing that Congress had no authority to regulate intrastate conduct. He recounted that he had taken the pictures in the

same state that he was apprehended in and since he had not distributed them to anyone out of state, the government had failed to prove that his conduct affected interstate commerce. Although the Court agreed with Bausch's recitation of the facts, it found that Congress had the power to regulate activities that substantially affects interstate commerce. Id. at pages 740-41. The Court found that since Bausch had used a Japanese camera to take the pictures and this camera had been transported in interstate or foreign commerce, his conviction was proper.

United States v. Wilson, 182 F.3d 737 (10th Cir. 1999). Conviction reversed where evidence was insufficient to support conclusion that diskettes in defendant's possession were materials that traveled in interstate commerce and were used to produce his graphic files.

United States v. Rodia, 194 F.3d 465 (3rd Cir. 1999). Defendant took photos using film which was manufactured outside of his state. Intrastate possession of child pornography was substantial effect on interstate commerce. Polaroid film creates sufficient "jurisdictional hook." But see United States v. Corp, 236 F.3d 325 (6th Cir. 2001). Held, in this particular case, not sufficient impact on Interstate Commerce to sustain conviction.

The government established a sufficient nexus between the activity described in an indictment charging a defendant with production of child pornography and interstate commerce to establish federal jurisdiction, where the defendant was involved in the type of child-exploitive and abusive behavior sought to be prohibitive in the applicable statute. The defendant forced two children under the age of 12, who were under his care and control, to view sexually explicit photos presumably transmitted over interstate lines, and then coerced them to engage in and photograph similar sexually explicit behavior, for the presumed purpose of transmitting those photographs in interstate commerce via computer. United States v. Andrews, 383 F.3d 374 (6th Cir. 2004).

Provisions of the Protection of Children Against Sexual Exploitation Act prohibiting sexual exploitation of children and possession of child pornography were unconstitutional under the Commerce Clause as applied to simple intra-state production and possession of images and visual depictions that were not mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, nor intended for interstate distribution or economic activity of any kind, including exchange of the pornographic recording for other prohibited material. Federal jurisdiction under the Commerce Clause could not be premised upon the fact that the camera used by defendant, and the tape medium upon which the images and sounds were recorded, previously had traveled in interstate and foreign commerce. United States v. Matthews, F. Supp. 2d 1220 (N.D.Ala. 2004).

The application of the federal statute prohibiting the knowing possession of child pornography to the intrastate possession of child pornography based entirely on the fact that the disks on which the pornography was copied traveled in interstate commerce before they contained the images violated the Commerce Clause. The defendant's activity was noneconomic and noncommercial in nature, its connection to interstate commerce was tenuous at best, the statute's jurisdictional element requiring the government to establish that the illegal images were produced by materials that were transported in interstate commerce did not ensure that the statute would be enforced only with regard to activity that has a substantial impact on interstate commerce, and the statute's legislative history provided no meaningful evidence that the intrastate possession of child pornography at issue, although produced with two disks that traveled in interstate commerce, substantially affected interstate commerce. United States v. Maxwell, 386 F.3d 1042 (11th Cir. 2004).

In 2005, the U.S. Court of Appeals for the Eleventh Circuit held that its decision in *Untied States v. Maxwell*, 386 F. 3d 1042, 76 CrL 20 (11th Cir. 2004), limiting prosecutors' ability to punish intrastate possession of child pornography as a federal crime, applies as well to intrastate production of child porn for personal use. Creating a circuit split, the court decided that the production of child pornography solely within one state – even with materials that have traveled in interstate commerce – does not have a substantial enough effect on interstate commerce to give rise to federal jurisdiction. (*United States v. Smith*, 459 F.3d 1276 (11th Cir. 2006).

It is a crime under 18 U.S.C. § 2251 (a) to use a minor to produce child pornography using materials that were transported in interstate commerce. The basis for federal jurisdiction at the defendant's trial was that the film, photo paper, and film processor used to produce the photos he made himself and kept in a lockbox at

his mother's home had traveled in interstate commerce before he used them to produce those images.

However, the U.S. Supreme Court granted *certiorari* in the *Smith* case, vacated the judgment and remanded the case for consideration in accordance with *Gonzales v. Raich*, 125 St. Ct. 2195 (2005).

Thereafter, in 2005 the 4th Circuit held that a Court did not commit error, much less plain error, in applying, to the defendant's wholly intrastate production and possession of child pornography, the federal statutes prohibiting the sexual exploitation of a minor for the purpose of producing child pornography [18 U.S.C.A. § 2251(a)] and prohibiting the possession of child pornography containing images transported in interstate commerce [18 U.S.C.A. § 2252A(a)(5)(B)]. In statutes, Congress "directly" regulated economic activity in a fungible commodity, namely, child pornography, by, inter alia, prohibiting its possession. Congress had a rational bases for concluding that the local production and possession of child pornography substantially affected interstate commerce, despite the *de minimis* character of individual instances arising under the statutes. *U.S. v. Forrest*, 429 F.3d 73 (4th Cir. 2005).

To obtain a conviction for the transportation of child pornography via computer, the government is not required to prove that the defendant knew that the channels of interstate commerce would be used when he shipped the offending images. Thus, evidence that the visual depictions of minors engaged in sexually explicit conduct which a defendant transmitted by electronic mail traveled from the defendant's home in Kentucky over the internet to California and Nova Scotia supported the defendant's conviction of the transportation of child pornography via computer, even if the defendant was unaware that interstate or foreign commerce would be used. *U.S. v. Chambers*, 441 F.3d 438 (6th Cir. 2006).

Production

It may be axiomatic to conceptualize that, for purposes of the statute, "production" occurs when a computer is used to download data. Lacy, 119 F.3d at 750. In prosecution for possessing images of child pornography on a computer hard drive that had been transported in interstate commerce, the Court of Appeals rejected the defendant's challenge to the sufficiency of the indictment. United States v. Anderson, 280 F.3d 1121 (7th Cir. 2002).

However, there has been an expansion of criminal liability for behavior beyond what is traditionally considered "production" to now include duplicating existing files - as opposed to creating images first hand by one who may be witnessing abuse. "Re-producing" is sufficient to satisfy the 18 U.S.C § 2252(a)(4)(B) issue allowing conviction for possessing an image that was "...*produced* using materials that traveled in interstate commerce". *U.S. v. Dickson*, 632 F.3d 186 (5th Cir. 2011).

Lasciviousness

Courts analyze the following factors to determine whether a visual depiction as a whole constitutes a "lascivious exhibition" under § 2256: "(1) whether the focal point of the visual depiction is the child's genitals or public area; (2) whether the setting of the image is sexually suggestive, *i.e.*, in a place or pose generally associated with sexual activity; (3) whether the child is depicted in an unnatural pose, or in inappropriate attire, considering the age of the child; (4) whether the child is fully or partially clothed, or nude; (5) whether the visual depiction suggests sexual coyness or a willingness to engage in sexual activity; [and] (6) whether the visual depiction is intended or designed to elicit a sexual response in the viewer." United States v. Dost, 636 F. Supp. 828, 832 (S.D. Cal. 1986), aff'd sub nom, United States v. Wiegand, 812 F.2d 1239 (9th Cir. 1987).

Visual depictions that focus on the genital and pubic area of minors may constitute "lascivious exhibitions" even when these body parts are covered by clothing and are not discernible. United States v. Knox, 32 F.3d 733 (3d Cir. 1994).

Mere nakedness is not a "lascivious exhibition." United States v. Amirault, 173 F.3d 28 (1st Cir. 1999) (using the Dost analysis to reverse the district court). Since this issue implicates First Amendment analysis, its resolution is subject to plenary review.

Photograph of 16-year-old boy was not "lascivious exhibition of the genitals" and thus did not constitute "sexually explicit conduct" within

meaning of statutes proscribing sexual exploitation of children. United States v. Boudreau, 250 F.3d 279 (5th Cir. 2001).

Post-production computer alterations of visual depictions of unclothed girls that placed pixel blocks over their genital areas did not take depictions outside reach of child pornography statute prohibiting knowing possession of visual depictions whose production involved use of a minor engaging in sexually explicit conduct and which depict such conduct; depictions remained a "lascivious exhibition." U.S.C.A. § 2252(a)(4)(B). United States v. Grimes, 244 F.3d 375 (5th Cir. 2001).

United States v. Rayl, 270 F.3d 709 (8th Cir. 2001). The question whether materials depict a "lascivious exhibition of the genitals" is for the finder of fact. However, the meaning of "lascivious exhibition of the genitals" is an issue of law. Court stated that the district court should conduct a preliminary review of whether the materials offered by the government depict sexually explicit conduct as a matter of law.

United States v. Kemmerling, 285 F.3d 644 (8th Cir. 2002). A picture is lascivious only if it is sexual in nature and intended to elicit a sexual response in the viewer.

Transmissions

In United States v. Matthews, 11 F. Supp. 2d 656, (D. Md. 1998), the defendant raised a multiplicity problem with his indictment. The defendant claimed that he should have been charged in two, rather than four, counts for his transmission of four e-mail attachments of pornographic images. He claimed that the images were part of only two on-line "conversations," each of which constituted a single use of the telephone wire, regardless of the number of transmissions made during each conversation. The court disagreed, holding that a defendant may be charged in separate counts for each e-mail transmission.

Miscellaneous

1. Crime of Violence

Possession of child pornography in violation of § 2252(a)(4) is a non-violent offense for purposes of a downward departure at sentencing. United States v. McBroom, 124 F.3d 533, 542 (3d Cir. 1997). *But see E below*, Pretrial Detention, below, regarding 18 U.S.C. § 3142(f).

2. Extraterritorial Application

A military court recently held that 18 U.S.C. § 2252(a)(2) applies extraterritorially, so that a lieutenant in the navy could be prosecuted for receiving child pornography while stationed in Japan. United States v. Kolly, 48 M.J. 795, 1998 WL 433688 (Navy-marine Ct. Crim. App., July 24, 1998).

3. Evidence Stipulation

A defendant could not exclude child pornographic images in a child pornography prosecution by offering to stipulate that the images were pornography within the statute. The evidence was factual not legal and rule in Old Chief did not apply. United States v. Campos, 221 F.3d 1143 (10th Cir. 2000).

Defendant objected to government showing pornographic films to jury when he was willing to stipulate that the films contained child pornography and had traveled interstate (only dispute was whether defendant knew materials depicted children engaged in sexually explicit conduct). District court overruled objection; Ninth Circuit reversed. United States v. Merino Balderrama, 146 F.3d 758 (9th Cir. 1998).

Allowing the jury, at their specific request, to view three of thirty-four exhibits was not unduly prejudicial. Unlike Merino-Balderrama, there was evidence that defendant had seen the images and the images were relevant to disprove defendant's defenses. United States v. Hay, 231 F.3d 630 (9th Cir. 2000).

Government sought to introduce small portion of 120 images found on defendant's computer and diskettes. Defendant argued that allowing the jury to view "highly inflammatory images that depict naked children engaged in sexual acts" was prejudicial in violation of FRE 403. District court held the images were the key to the charges, no improper propensity evidence. District court established rules for the manner in which the exhibits would be presented such as blocking out the genital portions of the images presented in open court. United States v. Dean, 135 F. Supp. 2d 207 (D.Me.2001).

Jury Instructions

See United States v. Kimbrough, 69 F.3d 723 (5th Cir. 1995), where the Fifth Circuit approved the submission of instructions regarding a violation of section 2252(a).

Also see, United States v. Crow, 164 F.3d 229 (5th Cir. 1999), regarding §§ 2251 and 2252.

District court did not abuse its discretion in refusing defendant's requested instruction that illicit sex must have been one of his dominant purposes for foreign travel in order to convict for traveling in foreign commerce for the purpose of engaging in a sexual act with a juvenile. 18 U.S.C. § 2423(b). United States v. Garcia-Lopez, 234 F.3d 217 (5th Cir. 2000).

The Court affirmed convictions and sentences for a defendant convicted of transporting child pornography in interstate commerce in violation of 18 U.S.C. §§ 2252A(a)(1) and 2252A(a)(5)(B). The Court addressed the argument that the trial court committed reversible error when it gave a jury instruction that allowed the jury to convict even if the images involved "virtual" as opposed to "actual" children, in violation fo the holding that convictions for "virtual" images infringe on the First Amendment under Ashcroft v. Free Speech Coalition, 122 S.Ct. 1389 (2002). Reviewing the matter for "plain error," the Court found that the instruction was in error and that the error was "plain," but found that it did not seriously affect the fairness, integrity or public reputation of judicial proceedings because the evidence clearly established that actual, not virtual, children were depicted in Richardson's images. United States v. Richardson, 304 F.3d 1061 (11th Cir. 2002).

Duplicative Charging

Where defendants owned a number of websites that transmitted hundreds of images of child pornography, court found that "rule of lenity" required that defendants be charge only with the websites themselves, and not with each individual image that was transmitted. United States v. Reedy, 304 F.3d 358(5th Cir. 2002).

D. Constitutional Issues and Case Law

1. Constitutional Challenges

The constitutional definition of "obscenity," was solidified in Roth v. United States, 354 U.S. 476 (1957). The Roth definition asks if the material deals with sex in a manner appealing to prurient interests. This standard was further explained in Miller v. California, 413 U.S. 15 (1973), a case which explored the constitutionality of a state statute prohibiting the mailing of unsolicited sexually explicit material. The court expressed the test of obscenity as:

(a) whether the average person, applying community standards would find that the work, taken as a whole, appeals to the prurient interest,

(b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and

(c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

Miller addressed the issue of adult pornography, not child pornography. Although the Miller Court held that the distribution of obscene materials can be regulated, in a prior case, Stanley v. Georgia, 394 U.S.C. 557, the Court held that the private possession of obscenity cannot be proscribed. This ruling was based on a person's right to privacy in his or her own home, and the issue of the First Amendment was not paramount. The Court, in Stanley, held that, not withstanding the government's right to regulate the distribution of obscene materials, it does not have the right to control the moral content of a person's thoughts. The Court reasoned that the government may not prohibit the mere possession of obscene material on the grounds that it may lead to antisocial conduct.

In 1982, the U.S. Supreme Court in New York v. Ferber, 458 U.S. 747 (1982), created a new category of unprotected speech: child pornography. In Ferber, the Court held that the

evils involved in producing child pornography, namely the sexual abuse of children, caused the material to fall outside the protection of the First Amendment. The government, therefore, met its strict scrutiny burden of proof. New York's interest in preventing child sexual abuse at the hands of child pornographers was compelling enough to allow the banning of child pornography.

The Ferber decision empowered states to enact laws to combat the child pornography industry. The enforcement of these laws is not hindered by the constitutional attacks based on the First Amendment issues involved in laws regulating obscenity, because child pornography may be made illegal per se, without nay proof that the material is obscene. Child pornography has been defined as photographs of actual children engaged in some sort of sexual activity, either with adults or with other children. Child pornography, of course, includes still photographs, but it may also take the form of videos, or still photographs that have been scanned into a computer image. However, child pornography does not include hand-made drawings, sculptures, or graphic written accounts of sex with children. In order to understand a legal analysis of the constitutional issues of virtual child pornography, it is important to note that, until very recently, child pornography, by definition, required pedophiles to sexually exploit children in order to create the materials.

In the Internet age, the application of the Miller "community standard" presents an interesting challenge. The Sixth Circuit recently rejected a "cyberspace community standard" in favor of a local Memphis, Tennessee community standard in testing the obscenity of material downloaded onto a computer in Tennessee, but posted on an electronic bulletin board located in California. United States v. Thomas, 74 F.3d 701 (6th Cir.).

The possession and viewing of child pornography are not entitled to First Amendment protection because the government has a compelling interest in protecting the physical and psychological well-being of exploited minors. Osborne v. Ohio, 495 U.S. 103 (1990).

2. Communications Decency Act of 1996 (the "CDA") and Child Online Protection Act (COPA)

The Supreme Court has ruled that two provisions of the CDA - aimed at protecting children from "indecent transmissions" and "patently offensive displays" on the Internet -- were unconstitutionally vague and over broad in violation of the First Amendment. Reno v. American Civil Liberties Union, 117 S.Ct. 2329 (1997). Negligence action brought against America Online (AOL) on the ground that it unreasonably delayed in removing, failing to screen for, and failing to post retractions of defamatory messages, held barred by the CDA. Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997).

Following the ruling in Reno, Congress went back to the drawing board and came up with The Child Online Protection Act (COPA), which makes it a crime punishable by fine or imprisonment for a web site operator to "knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, make [ ] any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors" is defined in Section 231(e)(6) by a three-pronged test that tracks the Miller obscenity test, including whether "the average person, applying contemporary community standards, would find [that the material, taken] as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest." An affirmative defense is offered for those web sites that take steps to screen out Internet users under age 17.

The Child Online Protection Act (COPA) of 1998 is not unconstitutionally over broad just because it uses a "community standards" test like that from Miller v. California, 413 U.S. 15 (1973), to regulate speech on the World Wide Web. Ashcroft v. American Civil Liberties Union, 122 S.Ct. 1700,1713 (2002). The court, however, was deeply divided on how Congress may regulate speech on the Web.

However, on March 6, 2003, the United States District Court of Appeals for the Third Circuit again held that the COPA of 1998 is unconstitutional. This time around, the Third Circuit took up two arguments for finding COPA unconstitutional that it had not addressed in its first opinion: the law fails to satisfy the First Amendment's "strict scrutiny" standard for content-based restrictions on speech and it prohibits a substantial amount of speech protected under the First Amendment. In the court's view,

COPA failed both inquiries. *American Civil Liberties Uniton v. Ashcroft*, 322 F.3d 240 (3d Cir. 2003). On October 14, 2003, the United States Supreme Court granted a petition for certiorari to review the case in no. 03-218.

On March 20, 2006, the United States Supreme Court summarily affirmed a decision of a three-judge panel of the Untied States District Court for the Southern District of New York that an obscenity provision of the Communications Decency Act (CDA) was not over broad in violation of the First Amendment. The provision in question, 47 U.S.C.A. § 223 (a)(1)(B), makes it a crime, inter alia, knowingly to transmit obscenity by means of the Internet to a minor. The declaratory-judgment action was brought by an art photographer and a nonprofit organization whose members' noncommercial websites displayed images of adults engaged in nontraditional sexual practices. The action was referred to a three-judge panel pursuant to the CDA.

3. Child Pornography Prevention Act (the "CPPA")

A. Historical Perspective

In 1997, a federal district judge in California upheld the constitutionality of the CPPA against a First and Fifth Amendment challenge. The plaintiffs argued that the CPPA's prohibition of images that *appear* to be of children actually criminalizes the production and sale of legitimate works. The Court disagreed. It held that the CPPA is content-neutral and advances compelling governmental interests because it was enacted to address the effects child pornography has on society and innocent children, rather than to regulate the ideas expressed in the pictures. It also noted that the affirmative defense in § 2252A(c) would be available to producers or distributors of such legitimate works. Free Speech Coalition v. Reno, No. C 97-0281 VSC, 1997 WL 487758 (N.D. Cal. Aug. 12, 1997).

Thereafter, in The Free Speech Coalition v. Reno, 198 F.3d 1083 (9th Cir. 1999) (petition for rehearing denied July 24, 2000). The court said: "We find that the phrases 'appears to be' a minor, and 'convey the impression' that the depiction portrays a minor, are vague and over broad and thus do not meet the requirements of the First Amendment." The court said the balance of the Child Pornography Prevention Act, or CPPA, was constitutional when those phrases are removed.

A federal district court in the First Circuit considered another First Amendment challenge to the CPPA in the context of a criminal prosecution. Although the court rejected the defendant's argument that the CPPA prohibited constitutionally protected speech, the court did agree that the CPPA is unconstitutionally vague and over broad in violation of the First Amendment. The Court held that the CPPA's broadened definition of "child pornography," which includes materials that "appear to be" of children, is vague because it fails to adequately warn viewers of what conduct is prohibited. The definition is also over broad because it sweeps within its scope a substantial amount of constitutionally-protected pornography featuring younger-looking adults. United States v. Hilton, Criminal No. 97-78-P-C (D. Me. Mar. 30, 1998).

However, on January 27, 1999, the First Circuit Court of Appeals held that 18 U.S.C. § 2252 is neither vague nor invalid under the First Amendment. The conduct reached by the statute is outside the protection of the free speech guarantee, and the prohibition of images that "appear [] to be" of minors is sufficiently clear to satisfy due process concerns, the court said. (United States v. Hilton, CA1, No. 98-1513, 1/27/99, reversing 999 F. Supp. 131, 63 CrL 85). A Motion for Rehearing was denied in March 1999. On May 28, 1999 a Petition for Certiorari was filed with the U.S. Supreme Court. The petition was denied on October 4, 1999.

On March 6, 2000, the District Court for the Northern Division of Utah held the CPPA constitutional. A Defendant charged with various child pornography offenses moved to dismiss multiple counts, asserting that Child Pornography Protection Act (CPPA) was unconstitutional for vagueness, over breadth, and burden-shifting. The District Court, Stewart, J., held that: (1) the scrutiny of Act was required; (2) as a matter of first impression, Act's prohibition of computer-generated pornography appearing to involve minors was not over broad or vague under the First Amendment; and (3) Act's affirmative defense permitting proof of subject's adulthood was not improper burden-shifting. United States v. Pearl, 89 F. Supp. 2d 1237 (D. Utah 2000).

Also see United States v. Fiscus, 105 F. Supp. 2d 1219 (D. Utah 2000). Child Pornography Prevention Act (18 U.S.C. § 2252A), definition of the crime as a visual depiction that "appears to be" or "conveys impression" of a

minor engaging in sexually explicit conduct is not unconstitutionally vague or over broad.

Prosecution of a pedophile pursuant to § 2252 is not unconstitutional under the Eighth Amendment. United States v. Black, 116 F.3d 198 (7th Cir.).

B. Ashcroft v. Free Speech Coalition

On April 16, 2002, the United States Supreme Court held by a vote of 7-2 (majority opinion by Kennedy, concurrences by Thomas and O'Connor; dissents by O'Connor, Scalia and Rehnquist) that the sections of the Child Pornography Prevention Act that prohibit computer-generated images that appear to be minors engaging in sexually explicit conduct are unconstitutionally broad.

The Child Pornography Prevention Act of 1996 (CPPA) expanded the prohibition on child pornography to include computer-generated images "that appear to be" minors engaging in sexually explicit conduct. The Act bans any explicit material produced or distributed that panders child pornography. Respondents, including an adult-entertainment trade association, filed suit alleging the provisions were over broad, vague and unconstitutional under the First Amendment. The District Court granted the government summary judgment and the United States Ninth Circuit Court of Appeals reversed and held the CPPA facially invalid. The United States Supreme Court affirmed as to two provisions, holding that these CPPA provisions were too broad because they unconstitutionally banned a substantial amount of protected speech. The Court reasoned that the CPPA prohibited speech without regard to whether it appealed to the prurient interest, was patently offensive, or had any serious redeeming value. The Court distinguished New York v. Ferber, 458 U.S. 747 (1982), from the CPPA's prohibition on speech that did not exploit any children in the production process. The Court also held that the section that made knowingly possessing mislabeled prohibited material a crime was too broad to be constitutional.

The majority rejected the government's argument that the statute's broad sweep is necessary to stop pedophiles from using virtual child pornography to seduce children or to whet their own sexual appetites. Those justifications are insufficient to ban speech fit for adults, it said. In addition, because the statute does not incorporate the "community standards" test of obscenity requiring that the artistic merit of a work be judged considering the work as a whole, it could be used to prosecute makers and possessors of popular films such as "Traffic" and "American Beauty" that have even a single scene depicting teenage sex, the majority said.

The argument that virtual child pornography may be used to seduce children fails, the majority said, because the government "cannot ban speech fit for adults simply because it may fall into the hands of children." The claim that virtual child pornography might whet pedophiles' appetites likewise fails, the majority said, because the government "cannot constitutionally premise legislation on the desirability of controlling a person's private thoughts."

The government also argued that producing child pornography using computer imaging makes it difficult to prosecute those who produce pornography using actual children because experts may have difficulty saying whether the pictures were made using real children or computer imaging. But the majority said this argument "turns the First Amendment upside down" by allowing the government to ban protected speech as a means to ban unprotected speech.

E. Pretrial Detention

Title 18 U.S.C. § 3141 et seq., sets forth the controlling statutes on the issue of pretrial release or detention. These sections provide certain circumstances under which the government may seek to have a person detained without bond pending trial. 18 U.S.C. § 3142(f).

The government may move for a detention hearing where the case involves:

1. a crime of violence;
2. an offense for which the maximum sentence is life imprisonment or death;
3. a drug offense carrying a maximum term of imprisonment of ten years or more;
4. any felony committed after the person has been convicted of two or more of the above offenses

(state or federal);

5. a serious risk of flight;

6. a serious risk that the person will obstruct or attempt to obstruct justice or threaten, injure or intimidate or attempt to do so to a prospective witness or juror.

A crime of violence is defined in 18 U.S.C. § 3156(a)(4) as follows:

(A) an offense that has as an element of the offense the use, attempted use, or threatened use of physical force against the person or property of another;

(B) any other offense that is a felony and that, by its nature, involves a substantial risk that physical force against the person or property of another may be used in the course of committing the offense; or

(c) any felony under Chapter 109A or Chapter 110.

Title 18 U.S.C. §§ 2551 through 2252A are felonies under Chapter 110.

However, can a person be released under 18 U.S.C. § 3145 (c) pursuant to the "exceptional reasons" clause? Title 18 U.S.C. § 3145(c) provides that "a person subject to detention pursuant to section 3143(a)(2) or (b)(2), and who meets the conditions of release set forth in §3143(a)(1) or (b)(1), may be ordered released, under appropriate conditions, by the judicial officer, if it is clearly shown that there are exceptional reasons why such person's detention would not be appropriate."

The language of the sentence included in § 3145(c) is direct. It states that "the judicial officer" may order release if certain conditions are met and there are exceptional reasons why detention would be inappropriate.

Section 3143(a)(2) supplies the threshold requirements that a person convicted of a "violent crime" must meet. To satisfy those requirements, the trial judge must find that the person poses no risk of flight and no danger to the community during release. 18 U.S.C. § 3143(a)(2). Only then does the trial court consider the presence of exceptional circumstances making detention inappropriate. See United States v. Carr, 947 F.2d 1239, 1240 (5th Cir. 1991) (per curiam) (exceptional reasons provision to be applied on original application despite inclusion of provision "in a section generally covering appeals."); United States v. Douglas, 824 F. Supp. 98, 99 (N.D. Tex. 1993).

Neither the statute nor case law defines the circumstances that may qualify as exceptional reasons permitting release. There is sparse case law regarding the factors that the district court must consider in deciding the issue of whether there are exceptional reasons why such person's detention would not be appropriate. The Court of Appeals for the Ninth Circuit stated in United States v. Koon, 6 F.3d 561 (9th Cir. 1993), that "whether 'exceptional reasons' exist must be determined case-by-case." The Second Circuit offers a working definition of "exceptional reasons:" "a unique combination of circumstances giving rise to situations that are out of the ordinary." United States v. DiSomma, 951 F.2d 494, 497 (2d Cir. 1991). Another court notes that "purely personal considerations" such as disruption of the family do not constitute exceptional reasons within the meaning of 18 U.S.C. § 3145(c) because "[a] defendant's incarceration regularly creates difficulties for him and his family." United States v. Mahabir, 858 F. Supp. 504, 508 (D. Md. 1994). See also, e.g., United States v. Douglas, 824 F. Supp. 98 (N.D. Tex. 1993) (finding fact that defendant had pled guilty to cocaine trafficking charge and agreed to cooperate with the government by testifying against codefendants, leaving himself open to retaliation, not sufficient to qualify as "exceptional reasons"); United States v. Bloomer, 791 F. Supp. 100 (D.Vt. 1992) (finding defendant's close relationship with his stepchild, his financial support of the family, his support to an unrelated family, and his health problems stemming from his affliction with cerebral palsy not sufficient to qualify as "exceptional reasons"); United States v. Taliaferro, 779 F.Supp. 836 (E.D. Va.1992), aff'd, 993 F.2d 1541 (4th Cir.).

Pretrial Release-Distribution / Transportation: Electronic Monitoring Required.

It is also an enormous practical concern for those individuals charged with distribution or transportation *[not simple possession]* of child pornography that section 216 of the Adam Walsh

Act modified 18 U.S.C. 3142(c)(1)(B) to now require, at a minimum, imposition of electronic monitoring for anyone fortunate enough to gain pre-trial release on those charges.

F. Pretrial Hearings, Discovery, and Government Discovery Violations

The defense may decide to request a pretrial hearing at which the government must prove the image involved does depict a minor, and not merely a synthetic image resembling a minor. Ashcroft v. Free Speech Coalition, 122 S.Ct. 1389 (2002).

Support for such a hearing can be found in Fort Wayne Books, Inc. v. Indiana, 489 U.S. 46, 67 (1989). But see Lamb, 945 F. Supp 441, 454-55 (N.D.N.Y. 1996) (declining to hold such a hearing). In Fort Wayne Books, the Supreme Court held that in an obscenity/RICO prosecution of an adult bookstore, the state had to show at an adversarial pre-trial hearing that the materials seized pursuant to a warrant were obscene. The *ex parte* probable cause determination, which resulted in the issuance of the seizure warrant, was insufficient to sustain the pretrial seizure of the bookstore's inventory. The Court reasoned that it was necessary to prevent presumptively protected materials from being removed from circulation without the protection of an adversarial hearing. Fort Wayne Books, 489 U.S. at 62-67; see also Adult Video Ass'n v. Barr, 960 F.2d 781, 788 (9th Cir. 1992) (citing Fort Wayne Books, 489 U.S. at 66), vacated sub nom., Reno v. Adult Video Ass'n, 509 U.S. 917 (1993), modified in part, 41 F.3d 503 (9th Cir. 1994),.

Of course, this argument in favor of a pretrial hearing had considerable force in Fort Wayne Books and Adult Video Ass'n when it applied to the wholesale seizure of a business's inventory as a result of an allegation that the inventory contained some child pornography. Nevertheless, the defense should consider arguing that a citizen's right to view sexually explicit materials in private is no less deserving of First Amendment protection than a business's right to sell materials for a profit. If a pretrial adversarial hearing is necessary to protect the profits of a business, it should be just as necessary to protect the rights of an individual.

A discovery issue in a computer child pornography case may be whether the defense is allowed access to the alleged contraband. U.S. Attorney offices may oppose providing defense counsel with copies of any alleged contraband images based upon United States v. Kimbrough, 69 F.3d 723 (5th Cir. 1995). The stated rationale for this position is the government's refusal to participate in further "exploitation" of the child through further dissemination of the image. In actuality, the government means that it is acceptable for the prosecutor as well as the case agent to have the images, but not for defense counsel. The government only allows defense counsel and defense experts to view the images at the prosecutor's or case agent's office, or the prosecutor offers to have the case agent bring the images via computer disk to the defense expert while maintaining a vigil over the image's whereabouts.

An obvious line of response to such a situation is to file a motion with the trial judge under Rule 16 of the Federal Rules of Criminal Procedure. Such images are discoverable under one of the three bases of that rule: (1) as tangible items either seized from or belonging to your client; (2) as material necessary to the preparation of the defense; or (3) as material the government intends to use at trial. Additionally, the defense attorney should be prepared to argue that the constitutional right to counsel, a fair trial, and due process require the production of the images to the defense without a case agent "babysitter" being present.

Despite the seeming obviousness for the need to produce the images to the defense, the trial judge may need to be convinced. Therefore, you must be prepared to educate the judge on how computerized images are created and stored. An affidavit from an expert or live testimony may be necessary.

Practice Note:

ADAM WALSH CHILD PROTECTION AND SAFETY ACT OF 2006 (H.R. 4472)

On July 27, 2006, President Bush signed H.R. 4472. It provides as follows:

Section 604. Prevention of Distribution of Child Pornography Used as Evidence in prosecutions.

Section 3509 of Title 18 United States Code is amended by adding at the end of the following:

Prohibition on Reproduction of Child

Pornography –

"(1) In any criminal proceeding, any property or material that constitutes child pornography (as defined by section 2256 of this title) must remain in the care, custody, and control of either the Government or the court.

"(2)(A) Notwithstanding Rule 16 of the Federal Rules of Criminal Procedure, a court shall deny, in any criminal proceeding, any request by the defendant to copy, photograph, duplicate, or otherwise reproduce any property or material that constitutes child pornography (as defined by section 2256 of this title, so long as the Government makes the property or material reasonably available to the defendant.

"(B) For the purposes of subparagraph (A), property or material shall be deemed to be reasonably available to the defendant if the Government provides ample opportunity for inspection, viewing, and examination at a Government facility of the property or material by the defendant, his or her attorney, aid any individual the defendant may seek to qualify to furnish expert testimony at trial."

In addition, defense counsel will want a copy of all hard drives and floppies seized from the client regardless of whether the government alleges they contain pornography. This will become important to investigate defenses such as whether someone else had access to the computer other that their client or whether the contraband image was e-mailed to the client without his knowledge.

In a criminal case for possession of child pornography, the state of Texas conceded that it had committed several errors in copying the content of the defendant's hard drive. *Taylor v. State*, 93 S.W.3d 487 (Tex. App.–Texarkana 2002). Errors included not transferring the data onto a new or clean hard drive, but rather onto a hard drive that had been used in prior child pornography cases. Despite this, the trial court refused to grant the defendant access to a copy of the hard drive for independent analysis.

On appeal, defense counsel argued that the trial court's refusal to order the prosecution to provide him with a complete copy of the hard drive as "material physical evidence" for inspection required reversal. The appellate court agreed. Likening the situation to a drug case in which the defendant has the right to have the contraband reviewed by an independent expert , the appellate court stated, "mere inspection of the images...is not the same as an inspection of the drive itself (or an exact copy thereof). It is certainly not the same as an independent forensic examination of the contents of the hard drive by an expert." The appellate court ordered that an exact copy of the hard drive should have been produced for review by the defendant's expert. The conviction was reversed and the case remanded for a new trial.

A defendant, charged with receiving and/or possessing child pornography, was entitled to obtain copies of images seized from his computer to enable his counsel to investigate how and when the images came to appear and be accessed on his computer. There was no reason to think that the defendant's counsel or her expert could not be trusted to abide by a proposed protective order, which could also address the government's concerns about the risk of further dissemination. Moreover, the government's concern about re-victimization would be implicated regardless of where the defendant's counsel and her expert viewed the images. United States v. Frabizio, 341 F. Supp. 2d 47 (D. Mass. 2004).

However, in U.S. v. Jarman, the Court ordered the United States to produce a mirror image of the computer hard drive for forensic examination by the defense expert. This is an important ruling for the Defendant with obvious *Adam Walsh Act* implications that has yet to work its way through the Court system.

In United States v. Katz, 178 F.3d 368 (5th Cir. 1999), the Government brought an interlocutory appeal of a pretrial ruling excluding evidence in a criminal prosecution that charged Katz with a violation of 18 U.S.C. § 2252(a)(2), receipt of child pornography. The Government challenged the district court's ruling excluding the color versions of the GIF images. The district court found that the government's failure to disclose the "photographs" to the defendant in the identical form it intended to produce them at trial was either an attempt to "sandbag" the defense or highly unprofessional conduct and therefore limited the government to the use of black and white images. The court affirmed the exclusion of the images.

G Search and Seizure

Most possession of child pornography cases involve 4th Amendment search and seizure issues that are not entirely unlike any other criminal case that involves the search of a defendant's home or business. However, the computerized nature of a child pornography case adds a dimension to the issue. Potential issues include wiretap warrants and whether the government followed the correct legal procedures for obtaining a defendant's subscription information from an Internet service provider.

Important note: The latest revision (2009) of the Department of Justice manual entitled "Searching and Seizing Computers and Obtaining Electronic Evidence Manual" is available at the web site of the Computer Crime and IP Section of DOJ's Criminal Division: http://www.cybercrime.gov/ssmanual/.

Read this case!: A district court in Connecticut has published a decision that offers a very detailed analysis of the Fourth Amendment implications of government searches of a seized computer. In United States v. Triumph Capital Group, Inc, 211 F.R.D. 31 (D. Conn. 2002). (Nevas, J.), the court held that while the Fourth Amendment's "reasonableness" standard should be the guide, careful judicial scrutiny of the process is required. Orin S. Kerr, associate professor at George Washington University Law School, discussed the case on his web site, hermes.circ.gwu.edu/archives/cybercrime.html.

Pursuant to the balancing test set forth in U.S. v. Knights, a probationer's home computer was subject to a warrantless search by probation officers based on reasonable suspicion, even though his probation agreement did not contain a provision explicitly requiring him to submit to warrantless searches, the Eleventh Circuit has held. The crime for which the probationer was on probation involved possession of child pornography. The probationer's expectation of privacy in his computer and computer-related activities was reduced by a probation condition prohibiting him from using the Internet unless work-related and during work hours. The probationer's expectation of privacy was further reduced because of his actions while on probation, which included several violations of the terms of his release and several times in which he placed himself in situations that were inappropriate for a convicted child sex offender. These actions justified the probation officers in monitoring him more closely and imposing greater infringements on his privacy. U.S. v. Yuknavich, 419 F.3d 1302 (11th Cir. 2005).

Denying *certiorari*, the United States Supreme Court has let stand a ruling of the Second Circuit Court of Appeals that agents had probable cause to search the home of a defendant based on his joining an Internet e-group that has members who exchanged child-pornography, although there was no evidence that defendant had ever downloaded any illegal visual depictions from the website.

Although it affirmed the denial of the defendant's motion to suppress and child pornography conviction, the panel acted on basis that it was bound by another panel's earlier decision in U.S. v. Martin, 426 F.3d 68 (2d Cir. 2005), cert. Denied, 2006 of a similar search based on membership in another e-group. (See separate coverage for Martin v. U.S., Docket No. 05-1073, on which the Court also denied certiorari.) Coreas v. U.S., 126 S. Ct. 2861 (2006). A law enforcement officer's averment in a search warrant affidavit that the target possessed images that appeared to depict a "prepubescent boy lasciviously displaying his genitals" was not sufficient to establish probable cause to believe that the materials were child pornography. The affidavit's language, unaccompanied by samples of the images or descriptions of them, was nothing more than a bare assertion about the legal status of the images. The court went on, however, to determine that the evidence could be admitted pursuant to the good-faith exception to the exclusionary rule. The court warned, however, that after this opinion, an agent's choice to withhold photos from a judicial officer in this sort of case will be viewed differently. United States v. Brunette, 256 F.3d 14 (1st. Cir. 2001).

A federal agency official's investigation of alleged criminal activity by a federal employee does not invalidate the warrantless seizure of computer discs under the workplace efficiency doctrine of O'Connor v. Ortega. United States v. Reilly, No. 01 CR 1114, 2002 WL 31307170 (S.D.N.Y. June 6, 2002). The seizure of the diskettes was permissible under an exception to general Fourth Amendment requirements for searches, which gives agencies leeway to maintain order in the workplace, the court said.

On August 5, 2002, in a case of apparent first impression, the U.S. District Court for the District of Puerto Rico held that the defendant

lacked a constitutionally-protected privacy right in a photograph of himself that had been posted on an Internet web site, United States v. Gines-Perez, 214 F. Supp. 2d 295 (D. Puerto Rico 2002). The court said it did not matter, for Fourth Amendment purposes, that the web site was "under construction" or that the contents of the site were in any sense considered by the defendant to be private.

FBI agents violated the Fourth Amendment rights of a suspect when they relied on the consent of a third party who shared a computer with the suspect to search the suspect's password-protected computer files. Password-protected files on a shared computer are analogous to a locked footlocker left in a shared living space. Trulock v. Freeh, 275 F.3d 391 (4th Cir. 2001).

United States v. Runyan, 275 F.3d 449 (5th Cir. 2001) held that: (1) removal by defendant's wife of child pornography from defendant's ranch constituted private "search" for purposes of Fourth Amendment; (2) police officers exceeded scope of such private search when they failed to confine their examination of computer disks to those disks that wife had examined; and (3) with respect to disks that wife had examined, officers did not exceed scope of her private search if they examined more files than she had examined.

United States v. Slanina, 283 F.3d 670 (5th Cir. 2002) held that: (1) defendant had reasonable expectation of privacy in files stored on his work computer; (2) O'connor exception to warrant requirement for work-related searches of public employees' space applied to search of computer for child pornography by supervisor who was also law enforcement official; (3) search was reasonable under O'connor.

Allegation in police officer's affidavit supporting issuance of warrant for search of home of defendant, a high school basketball coach, for adult pornography, that defendant engaged in a continuous pattern of sexual abuse and inappropriate conduct, had nothing to do with whether he continuously possessed and showed pornography to boys in his home, and did not establish any probable cause to search his home for adult pornography. United States v. Zimmerman, 277 F.3d 426 (3rd Cir. 2002).

Law enforcement did not make an illegal search by turning over a face-down paper that portrayed child pornography. The court held that the "plain view" doctrine applied; the officer could see through the white sheet of paper which portrayed a child in a sexual position. United States v. Simmonds, 262 F.3d 468 (5th Cir. 2001).

See United States v. Alvarez, 127 F.3d 372 (5th Cir. 1997), wherein the court found that in a § 2252(a)(4)(B) case that, a law enforcement officer's statement in an affidavit for a search warrant that a videotape possessed by the defendant depicted "sexual conduct" demonstrated reckless disregard for the truth.

Several federal judges have found that FBI agents who prepared search warrant affidavits in "operation candyman" acted with reckless disregard for the truth. The FBI claimed that anyone who had signed up to join the Internet group at the center of the investigation automatically received child pornography from other members through an e-mail list. The claim was used to obtain search warrants for the homes and computer of people who had joined the group, known as candyman. The Bureau later conceded that people who had signed up for the group – which also included chat sites, surveys and file sharing – opted out of the mailing list and did not automatically receive pornography. See United States v. Perez, 247 F. Supp. 2d 459 (S.D.N.Y. 2003), for an excellent in-depth discussion of the affidavit, the issues, and the candyman cases.

In United States v. Carey, 172 F.3d 1268 (10th Cir. 1999), the court reversed a conviction for possession of child pornography after police, who obtained a warrant to search defendant's computer files for drug related items, downloaded and viewed 44 image files. The police claimed inadvertent discovery after seeing the first pornographic image, but failed to get a warrant to look at the other files. The appeals court said that the police needed a second warrant to view the remaining image files.

United States v. Villard, 678 F. Supp. 483 (D.N.J. 1988), aff'd on other grounds, 885 F.2d 117 (3d Cir. 1989). Executing arrest warrant in Calif. for fed charges out of NJ (transp. child porn). Saw binder of pages of photographic slides on closet shelf. Held page of slides up to light, saw suspected child porn. Got search warrant to search apt.; held: evidence suppressed.

United States v. Hall, 142 F.3d 988 (7th Cir. 1998). During CPU repair/upgrade, tech saw unusually named files and viewed 4 - 6 files (1,000 files total). Tech called state trooper, describes 2 - 3 images; trooper had tech copy several of the files onto a disk. Held: evid. discovered by private search; government

conceded copying of files to disk was a warrantless search, but copied disk was never reviewed by law enforcement nor used as basis for probable cause in the search warrant.

United States v. Jasorka, 153 F.3d 58 (2nd Cir. 1998). Issuing magistrate did not look at the photos, but relied on the Customs agent's opinion that the photos contained a lascivious display of the genitals. Held: agent's reliance on magistrate's determination of warrant application for violation of § 2252, based on lascivious exhibition of the genitals, was reasonable (relying on the authority of Leon, 468 U.S. 897 (1984).

United States v. Barth, 26 F. Supp.2d 929 (W.D. Texas, 1998). Computer technician was not government actor for the 4th Amendment purposes when he found child pornography on computer he was fixing despite the fact he was C.I. in addition to his computer job; however, one government knows of or acquiesces in the intrusive conduct, and the private party intends to assist law enforcement, then it is a warrantless search.

Computer store employee was not acting as agent of government when, in removing temporary files from computer with permission of defendant's wife in course of repairing computer, he opened JPG files and discovered images of unclothed, young female children, and thus, store employee's actions were not subject to analysis under Fourth Amendment. United States v. Grimes, 244 F.3d 375 (5th Cir. 2001).

In United States v. Grosenheider, 200 F.3d 321 (5th Cir. 2000), it was held that: (1) even if police officer's search of computer hard-drive was illegal, evidence discovered in customs agent's subsequent search pursuant to warrant was admissible under independent source and inevitable discovery doctrines; (2) even if police officer's seizure of computer in repair shop was illegal, evidence was admissible based on customs agent's subsequent re-seizure of computer pursuant to warrant.

A search warrant affidavit established probable cause supporting a search of the business records of the internet services provider used by a defendant suspected of accessing child pornography. The defendant had used his screen name and account with the provider to establish account with at least three suspect websites containing child pornography, and to access two additional websites. In addition, searches at the defendant's home and business resulted in the seizure of files indicating that the defendant had used the provider's instant messenger service to receive, share, and/or download child pornography files. The affidavit, moreover, sought information pertaining to records, including log files, electronic images, screen names, and account information, that would reflect evidence of criminal activity. United States v. Wagers, 2004 WL 2339065 (E.D. Ky. 2004).

Officers were objectively unreasonable in applying for and executing search warrant for defendant's computers and residence, and thus the good faith exception did not apply to suppression of evidence, where investigating officers waited four months to apply for warrant for search of defendant's residence and computers after they discovered defendant's membership information regarding mixed adult pornography/child pornography website, officers had ample opportunity but failed to analyze server seized from owner of site to determine whether defendant had downloaded images, and officers failed to present other target-specific corroborating information linking defendant's two-month membership to website to his probable possession of child-pornography. United States v. Gourde, 382 F.3d 1003 (9th Cir. 2004).

All evidence found in house search conducted with anticipatory warrant that was constitutionally invalid for failure to list triggering event, and all statements made by suspect at time of search, were excludable, since all occurred either during illegal entry or as direct result of it, regardless of whether search ultimately might have been conducted in manner consistent with valid warrant application, and regardless of whether officers possessed curative documents during search. United States v. Grubbs ,377 F.3d 1072 (9th Cir. 2004).

Case involves a search-incident-to-arrest of an "electronic rolodex," a Palm device, or personal digital assistant. The Sixth Circuit allowed the warrantless search of an "electronic address book" to locate the address of a co-conspirator. United States v. Goree, 47 Fed. Appx. 706 (6th Cir. 2002).

Many computer child pornography cases involve a defendant who allegedly downloaded images from the Internet or received then via e-mail. The medium utilized in child pornography cases triggers special search and seizure procedures. E-mail, for instance, is an "electronic communication" for purposes of the federal wiretap act, 18 U.S.C. §§ 2510-2522 (the

"Wiretap Act"). Before government agents may intercept the content of an e-mail, they must follow the same procedures necessary to wiretap a telephone. This includes getting an intercept warrant. 18 U.S.C. § 2518. If the provisions of the law are not complied with, the evidence derived from the unlawful intercept is subject to suppression under § 2515. The statute further provides that the wiretap warrant, its supporting affidavit, and evidence obtained from the warrant must be produced prior to any trial or hearing where the material is to be used. § 2518(9). If a case involves the interception of the contents of an e-mail, then it is crucial that the defense attorney carefully review the applicable statute and case law in this area.

A different statute applies when the e-mail was not intercepted during its transmission, but was stored on some online service computer, like AOL. See Stored Wire and Electronic Communications and Transactional Records Access Act, Title II of the Electronic Communications Privacy Act of 1996, Pub. L. No. 99-508, 100 Stat. 1848, 1860 (1986) (codified at 18 U.S.C. §§ 2701-2709). This statute governs the seizure of the material as well as law enforcement access rights to subscriber information like a client's Internet "handle," telephone number, or length of subscription to the Internet service.

If the content of the e-mail has been stored in the service provider's system for 180 days or less, then the content of the e-mail is obtainable only through a search warrant. 18 U.S.C. § 2703(a). E-mails more than 180 days old or other types of subscriber information may be obtained any number of ways, including warrant or subpoena. § 2703(b) & (c). Noticeably lacking from this provision is statutory authority for the suppression of evidence obtained in violation of the statute. *Cf*, 18 U.S.C. 2516 (authorizing suppression of wiretap evidence). Accordingly, an aggrieved defendant must simply argue that the Fourth Amendment requires suppression of any information obtained in violation of the Act. See United States v. Kimbrough, 69 F.3d 723 (5th Cir. 1995), regarding a search warrant involving a Title 18 U.S.C. § 2252 offense.

Federal law enforcement agents did not violate either the Fourth Amendment or the federal wiretapping law by obtaining a search warrant authorizing installation of a "key logger" device on a defendant's personal computer and using the device to discover the passphrase to an encrypted file. United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2002). Important Note: § 1030 Electronic Surveillance: The Homeland Security Act of 2002, signed into law by President George W. Bush on November 26, 2002, expands authority for the sharing of wiretap and electronic surveillance information. Section 225 expands the circumstances under which law enforcement can use pen registers and trap-and-trace devices during emergency situations. Existing law, 18 U.S.C. § 3125(a)(1), allows law enforcement to install pen registers or trap and trace devices without first seeking a court order in emergencies involving either an immediate danger of death or serious bodily injury to any person, or conspiratorial activities characteristic of organized crime. Section 225 expands this authority to cover two other types of emergencies: "an immediate threat to a national security interest" and "an ongoing attack on a protected computer (as defined in 18 U.S.C. § 1030) that constitutes a crime punishable by a term of imprisonment greater than one year."

Section 225 also includes a controversial provision allowing an Internet service provider to disclose the content of electronic communications, such as e-mail, to any government agency if the ISP in "good faith" believes that the communication relates to information that involves the risk of death or serious physical injury. Current law restricts those who can receive such communications to law enforcement agencies. "Good faith" replaces "reasonableness" as the legal standard for ISPs to use in determining whether there is a danger.

H. Evidence: Medical Experts (Tanner Staging); Age of Child, Real Child

Medical Experts

If the case involves images depicting individuals who look like they might be teenagers, the government will probably attempt to prove that the person depicted is a minor by a method called "Tanner Staging." Under the method developed by Dr. J.M. Tanner, a pediatrician or pediatric endocrinologist will look at the image, specifically at secondary sexual characteristics like breast development and pubic hair growth. See generally, J.M. Tanner, *Growth at Adolescence* (2d ed. 1962). From that information, the doctor will then render an

opinion on the probable age range of the depicted individual. A defense expert is crucial in understanding Tanner Staging and confronting the government's expert. For example, does the image present enough information about the pertinent secondary sexual characteristic for a medically valid opinion? **Note**: See PEDIATRICS Vol. 102 No. 6 December 1998, pp. 1494 Misuse of Tanner Puberty Stages to Estimate Chronological Age (by Rosenbloom and Tanner) http:/www.ci.keene.nh.us/police/tanner%20scale.htm. The official website is: http://www.pediatrics.org/content/vol102/issue6/index.shtml. Click on Letters to the Editor. In can be obtained for free.

Another potential issue concerning Tanner Staging is whether it is admissible under Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993). For an excellent summary of the Daubert decision, see James G. Connell, III, *Challenging Scientific Evidence under* Daubert: *Scope, Procedure, and Discovery*, CJA Defense Journal, Winter 1996 at 1.

However, United States v. Katz, 178 F3d 368 (5th Cir. 1999), where the defendant filed a pretrial Daubert motion pursuant to Federal Rules of Evidence 104(a) and 702. The Court found that the Tanner Scale was a scientifically valid methodology. The defendant had contended that the Tanner Scale analysis could not be adequately performed on the images. The Court ruled that the images and expert testimony were admissible.

Age of Child

United States v. Anderton, 136 F.3d 747 (11th Cir. 1998). Medical doctor's opinion as to age of depicted children was sufficient to allow jury to receive the case. Also see: United States v. Broyles, 37 F.3d 1314 (8th Cir. 1994). Language used by defendant in correspondence ("teenies"; between the ages of 11 and 15, just developing; range could be as low as 6 to 8 but no higher than 15); Postal Inspector's professional and personal familiarity with child development; pediatrics professor's testimony. United States v. Long, 108 F.3d 1377 (6th Cir. 1997) (unpublished disposition). Even though defendant did not actually view the video tapes before his arrest, Court found there was sufficient evidence that he knew about the ages of the participants and about the type of conduct depicted, due to the descriptions of the videos, the jacket illustrations, and the warning on the order forms.

United States v. Katz, 178 F.3d 368 (5th Cir. 1999). Whether the age of an individual depicted in an image can be determined by a lay jury without the aid of an expert's testimony must be determined on a case by case basis.

NOTE: FRE 701 was amended effective December 1, 2000, and now prohibits the admission of lay opinion evidence if it is based on specialized knowledge within the scope of FRE 702 (Expert opinion evidence).

United States v. Pollard, 128 F. Supp. 2d 1104 (E.D. Tenn. 2001). Analysis of Daubert, Kumho Tire and FRE 702 as related to the admissibility of expert opinion of age of female depicted in videotape.

United States v. Rayl, 270 F.3d 709 (8th Cir. 2001). District court did not abuse its discretion in permitting experience pediatrician to testify as an expert as to the age of children in photos, magazine and video found in defendant's possession.

Proving Picture Depicts a Real Child

United States v. Sims, 220 F. Supp. 2d 1222 (D.N.M. 2002). Conviction reversed under 2252(a) where the government put forth no evidence that the images depicted actual minors, and in fact objected to the notion that it was required to do so.

United States v. Bender, 290 F.3d 1279 (11th Cir. 2002). In child pornography trial, pediatric expert testified as to the age of the child depicted and that "the photographs appeared to portray a real child." On appeal the Court summarily denied defendant's Free Speech claim and noted there was sufficient evidence that the images portrayed real children.

United States v. Morgan, 2002 WL 975154 (D.Me. 5/10/02). Defendant was allowed to withdraw his guilty plea after Free Speech ruling because the defendant may not have had time to determine whether the images were of real children. Generally, the court will consider five factors relevant to withdrawal: 1) whether plea was voluntary; 2) force of defendant's reason for change of plea; 3) timing of request; 4) whether defendant asserts actual innocence; 5) whether plea agreement had been reached.

United States v. Guagliardo, 278 F.3d 868

(9th Cir. 2002). In dicta, Court approved of method of satisfying requirement of proving "actual children" by proving images were published prior to computer image alteration/creation technology became commercially available.

United States v. Vig, 167 F.3d 443 (8th Cir. 1999). Court held that the images that were viewed by the jury which was in a position to draw its own independent conclusion as to whether real children were depicted. No evidence was introduced to the contrary.

United States v. Nolan, 818 F.2d 1015 (1st Cir. 1987). Defendant claimed that insufficient evidence supported his conviction in that government failed to introduce an expert witness on the authenticity of the photography. Government's doctor did testify that the "gestalt" of the images were consistent with that of real children. Court found that the evidence was sufficient.

United States v. Richardson, 304 F.3d 1061 (11th Cir. 2002). Despite unconstitutional jury instruction (jury was instructed on "appears to be" language in 2256(8)), court affirmed defendant's conviction where an FBI agent had testified at trial that based on the circuit court's own viewing of the images left "no doubt" in their minds that the images depicted real children. Court found that although there was error, there would be miscarriage of justice in affirming the conviction.

The government in a prosecution for receiving child pornography was not required to do more than present the images to the jury for a determination whether the depictions were of actual children. The supreme Court's decision in Ashcroft v. Free Speech Coalition, which required that the images involved in child pornography prosecutions be real as opposed to computer-generated images of children, did not obligate the government to present expert testimony to that effect or otherwise impose a heightened standard of proof. United States v. Farrelly, 389 F.3d 649 (6th Cir. 2004).

"Juries are still capable of distinguishing between real and virtual images; and admissibility remains within the province of the sound discretion of the trial judge." U.S. v. Kimler, 335 F.3d 1142 (10th Cir. 2003). Therefore, the government was not required to present any additional evidence or expert testimony to meet its burden of proof to show that the images downloaded by Slanina depicted real children, and not virtual children. United States v. Slanina, 359 F.3d 356, (5th Cir. 2004).

However, most, including the 5th Circuit, follow the interpretation of *Ashcroft* that there can be no prosecution for offenses if the evidence is that the images were of "virtual" child pornography. *U.S. v. McNealy*, 625 F.3d 858 (5th Cir. 2010).

I. Entrapment, Impossibility, and Other Defenses

Defenses for child pornography are few. The defense of accidentally downloading the image or receiving unsolicited images through E-mail is credible only if those images are the only ones found in the defendant's possession. What the government looks for in these cases is whether the defendant is a "collector" or has extensive files.

1. Affirmative Defenses

Number of Depictions

It is an affirmative defense to a charge of 18 U.S.C. § 2252(a)(4) that the defendant

> - possessed less than three matters containing any visual depiction proscribed by that paragraph
>
> - and that he promptly and in good faith, and without retaining or allowing any other person other than a law enforcement agency, to access any visual depiction or copy thereof -
>
> > Took reasonable steps to destroy each image, or
> >
> > Reported the matter to a law enforcement agency and afforded that agency access to each such image."

18 U.S.C. § 2252(c).

In defining three or more matters, the hard drive is considered one matter though it may contain many images. United States v. Lacy, 119 F.3d 742 (9th Cir. 1997). However, the Ninth Circuit in United States v. Fellows, 157 F.3d 1197 (9th Cir. 1998), stated that a "computer hard drive is much more similar to a library than a book; the hard drive can store literally thousands of documents and visual depictions. Each file within the hard drive is akin to a book or magazine

within that library." Id. at 1201. The 5th Circuit seems to have settled on the notion that a "matter" may be an object that contains more than one image for this purpose. U.S. v. Buchanan, 485 F.3d 274 (5th Cir. 2007) However, in United States v. Vig, 167 F.3d 443 (8th Cir. 1999), the Eighth Circuit held that computer image files are encompassed within the meaning of "other matter." Id. at 449.

Subject was an Adult

It is an affirmative defense to a charge of 18 U.S.C. § 2252A(1), (2), (3), or (4) that the alleged child pornography was produced using an actual person or persons engaging in sexual conduct who was an adult at the time the material was produced and that the defendant did not advertise, promote, present, describe or distribute the material in such a manner as to convey the impression that it is or contains a visual depiction of a minor engaging in sexually explicit conduct. See 18 U.S.C. § 2252A(c).

Good Faith Effort to Destroy or Report

It is also an affirmative defense to a charge of 18 U.S.C. § 2252A(5) that the defendant possessed less than three images of child pornography and that promptly and in good faith, and without retaining or allowing any other person other than a law enforcement agency, to access any image or copy and took reasonable steps to destroy each image or reported the matter to a law enforcement agency and afforded that agency access to each such image. See 18 U.S.C. § 2252A(c).

2. Entrapment

Mark Poehlman, an Air Force Officer, a cross-dresser, and foot-fetishist, sought the company of like-minded adults on the Internet. What he found, instead, were federal agents looking to catch child molesters. The government's actions did amount to entrapment. United States v. Mark Douglas Poehlman, 217 F.3d 692 (9th Cir. 2000).

Jacobson v. United States, 503 U.S. 540 (1992). Government did not establish that defendant has a predisposition, independent of government action, to receive child porn through the mail. Evidence showed that defendant was ready and willing to commit the crime only after government had engaged in 2 ½ years of undercover activity consisting of communications from fictitious organizations and persons attempting to convince defendant that he had the right, or should have the right, to engage in behavior prohibited by law.

United States v. Gamache, 156 F.3d 1 (1st Cir. 1998). Case reversed because judge failed to instruct the jury on entrapment.

United States v. Osborne, 935 F.2d 32 (4th Cir. 1991). Receipt case. Defendant failed to produce any evidence of lack of predisposition, which warranted dismissal of the entrapment defense prior to trial. Defendant had responded to advertisement, placed by postal inspector in video publication, with letter indicating his interest in purchasing "young girl (teenagers) videos." He received catalog offering 5 adult and 5 child pornographic videos for sale, and then ordered 2 child porn videos.

United States v. Harvey, 991 F.2d 981 (2nd Cir. 1993). Receipt case. Defendant's requests for catalog of material featuring "younger performers," "young performers," and "your youngest performers" were indirect requests for child porn sufficient for jury to find predisposition beyond a reasonable doubt. Defendant's prompt acceptance of government-sponsored invitation to buy child porn, as reflected in the order form, was sufficient for government to show defendant was predisposed to commit the crime.

United States v. Gifford, 17 F.3d 462 (1st Cir. 1994). Receipt case. Evidence comfortably supported conclusion that postal inspectors did not induce defendant to commit the crime, and thus did not entrap the defendant, by mailing open-ended solicitations to purchase pornographic materials depicting children. Solicitations made no appeal to the sympathy of any obviously reluctant person, and in fact, defendant was required to pay in advance to obtain any material that he deigned to order.

United States v. Gendron, 18 F.3d 955 (1st Cir. 1994). Receipt case. No entrapment where government mailed solicitations from sham companies, where solicitations did not progress from innocent lure to frank offer, did not (with one exception) appeal to any motive other than desire to see child pornography, did not claim to come from lobbying organization seeking removal of restraints and funding its efforts through pornographic catalogue sales, and did not ask defendant to commit crime as a matter of principle.

United States v. Byrd, 31 F.3d 1329 (5th Cir. 1994). Receipt case. Sufficient evidence of defendant's predisposition to commit offense, though defendant had been targeted by undercover Postal Service "sting" operation, given evidence of defendant's eager and prompt response to each government mailing, his preexisting possession of foreign sex education text containing pictures of children and sexually explicit questionnaire prepared for 9-year-old boys, testimony that he fondled his young foster sons and had possession of photos of foster sons.

Agent Posing as a Child:

1. United States v. Butler, 92 F.3d 960 (9th Cir. 1996). A sentencing case pursuant to a travel case conviction where agent posed as the child while communicating with the defendant.
2. United States v. Brockdorff, 992 F.Supp 22 (D.C. 1997). Travel case where agent posed as child. Discussion by court validating this investigative technique.
3. United States v. Smith, 749 F.2d 1568 (11th Cir. 1985). Case deals with fraud statute but may be applicable by analogy. Defendant need not cause a "real" victim to travel interstate commerce to violate § 2314; causing the travel of a government agent who poses as a victim is sufficient.

3. Impossibility Defense

When a law enforcement agent poses as a child in an online undercover operation, the defense of impossibility may become an issue. This is true especially if the alleged offense includes sex with a minor.

The Fifth Circuit considered impossibility as a defense to a federal charge of attempting to persuade and entice a minor to engage in criminal sexual activity, in violation of 18 U.S.C. § 2422(b). See United States v. Farner, 251 F.3d 310 (5th Cir. 2001). The court held that defense of legal impossibility did not apply to preclude conviction, despite fact that victim was adult female agent of the Federal Bureau of Investigation (FBI).

The court noted that the typical definition of "legal impossibility defense" is a situation when the actions that the defendant performs or sets in motion, even if fully carried out as he desires, would not constitute a crime. *See also* United States v. Barlow, 568 F.3d 215 (5th Cir.2009)

In United States v. Root, 296 F.3d 1222 (11th Cir. 2002), defendant traveled to have sex with 13-year-old girl who turned out to be a law enforcement officer. Court followed Fifth Circuit finding that the existence of an actual minor victim is not required in order to convict. (**Note**: Court also allowed a two-level enhancement for unduly influencing minor where a defendant was more than 10 years older than the fictional victim).

On May 10, 2006, the Third Circuit held that no actual minor victim need be involved for a defendant to be convicted either of attempting to persuade a minor to engage in criminal sexual activity, in violation of 18 U.S.C. § 2422, or of traveling in interstate commerce for the purpose of engaging in a criminal sexual act with a minor, in violation of 18 U.S.C. § 2423. Congress did not intend for the impossibility defense to apply in this context, the court said. (United States v. Tykarsky,446 F.3d 354 (3d Cir. 2006). The defendant used an Internet chat-room and e-mail to converse with an undercover agent whom he believed to be a 14 year old girl. The defendant explicitly described the sexual activities he hoped to perform with the fictitious minor. He eventually made arrangements to meet the minor at a motel and was arrested when he arrived. At his trial and on appeal he raised a legal impossibility defense that rested on the fact that no minor was actually involved.

Other circuit courts that have examined the issues raised by the defendant have focused on the common law rule that legal impossibility is a defense but factual impossibility is not. Two circuits have held that the absence of an actual minor in a Section 2422 prosecution is a matter of factual impossibility and held that a conviction under the attempt provision of the persuasion statute does not require the involvement of an actual minor. United States v. Farner, 251 F. 3d 510 (5th Cir. 2001), United State v. Sims, 428 F. 3d 945 (10th Cir. 2005).

In addition, the defendant before the Third Circuit relied upon two unpublished district

court opinions that concluded that the legislative history of Section 2422 indicates that the involvement of an actual minor is a prerequisite to conviction. These decisions relied on Congress's refusal to adopt a statutory amendment explicitly criminalizing "contact[ing]," for purposes of engaging in illegal sexual activity, a person "who has been represented" as being under 18.

4. The "Knowingly" Requirement of §2252.

The "knowingly" scienter requirement § 2252 applies not only to receives, but also to the sexually explicit nature of the material and to the age of the performer. United States v. X-Citement Video, Inc., 115 S.Ct. 464 (1994). Therefore, in a § 2252(a)(2) case, the government must not only prove that the defendant "knowingly received" a visual depiction, but also that the defendant knew that the material was sexually explicit and that the performers were minors. United States v. Cedelle, 89 F.3d 181, 185 (4th Cir. 1996). United States v. Crow, 164 F.3d 229 (5th Cir. 1999).

Photograph of 16-year-old boy was not "lascivious exhibition of the genitals" and thus did not constitute "sexually explicit conduct" within meaning of statutes proscribing sexual exploitation of children. United States v. Boudreau, 250 F.3d 279 (5th Cir. 2001).

Postproduction computer alterations of visual depictions of unclothed girls that placed pixel blocks over their genital areas did not take depictions outside reach of child pornography statute, which prohibits knowing possession of visual depictions whose production involved use of a minor engaging in sexually explicit conduct and which depict such conduct; depictions remained a "lascivious exhibition." U.S.C.A. § 2252(a)(4)(B). United States v. Grimes, 244 F.3d 375 (5th Cir. 2001).

However, note than under § 2251(a), "a defendant's awareness of the subject's minority is not an element of the offense." United States v. United States District Court for the Central District of California, 858 F.2d 534, 538 (9th Cir. 1998).

Note: Also see Section X(C)(5) above regarding *mens rea* and knowledge.

5. Sufficiency of the Evidence

The government may fail to prove lascivious exhibition of genitals or pubic area, pursuant to 18 U.S.C. § 2256(2)(E). Nudity alone does not fit this description. There must be an "exhibition" of the genital area and this exhibition must be lascivious. Horn, 187 F.3d at 789. Several jurisdictions have attempted to define this by the following criteria: when child is nude or partially clothed, when the focus of the depiction is the child's genitals or pubic area, when the image is intended to elicit a sexual response in the viewer, when the setting is sexually suggestive, when the child is inappropriately attired or unnaturally posed, when there is a suggestion of sexual coyness or willingness to engage in sexual behavior. See United States v. Dost, 636 F. Supp. 828, 832 (S.D. Cal. 1986), aff'd sub nom, United States v. Wiegand, 812 F.2d 1239 (9th Cir. 1987); United States v. Amirault, 173 F.3d 28, 31 (1st Cir. 1999); United States v. Villard, 885 F.2d 117, 122 (3d Cir. 1989).

Note: Also see Section X(C)(7) of the paper regarding definitions, elements, and jury instructions.

J. U.S. SENTENCING GUIDELINES

1. A Judge's Struggle

Using the screen name Big Thing, one defendant sent thousands of images of child pornography to people who answered his advertisement in an Internet chat room. A federal judge responded with a heavy sentence, 10 years in prison. But even as he handed down the penalty, Judge Gerard E. Lynch angrily denounced his own decision. "This is without question the worst case of my judicial career," he said. The "unjust and harmful" sentence, he added, "has the potential to do disastrous damage to someone who himself is not much more than a child." BigThing was an 18-year-old college freshman who lived with his mother in Puerto Rico and had no prior criminal record. His trial, at a time when federal judges are chafing against strict sentencing measures passed by Congress, was the culmination of an extraordinary courtroom collision between a judge and the law he is sworn to uphold. In the case, which has played out in the federal district court in Manhattan over the last two years, Judge Lynch

tried to prevent the teenager from receiving the 10-year minimum sentence require by law. He urged prosecutors to reconsider the charge or to plea bargain, which might allow Mr. Pabon to avoid the mandatory term. When all that failed, he took the highly unusual step of announcing that he would reveal in his instructions to jurors the sentence the defendant faced.

The prosecution cried foul; under the rules of trials, jurors are to base their verdict solely on the evidence. The prosecutors suggested that the judge was trying to provoke the jury into ignoring the facts and acquitting out of sympathy – in effect, encouraging an act of civil disobedience.

Judge Lynch, a former prosecutor himself, said that was not his intention but might not be a bad result. For him, the problem was the law, a measure Congress passed in 1996 requiring that anyone convicted of advertising child pornography be imprisoned at least 10 years, regardless of his age or record.

Tough sentencing laws have won wide political support in recent years, particularly as the Internet creates vast new arenas for spreading pornography and victimizing children. Those laws have angered federal judges who see the mandatory penalties and sentencing guidelines as infringements on their authority, leading some to speak out, and in one case, resign. Then Chief Justice William H. Rehnquist ultimately criticized the special scrutiny given to Federal sentences that fell short of Congressional guidelines.

Judge Lynch, in the end, bowed to the law. He said he was not out to make the trial "some kind of cause celebre." He has decline to speak publicly about the case and it received little publicity.

The dispute, which continued in appeals, offers a rare look at how a judge tried to maneuver between lawmakers' command that he punish all criminals of a particular class the same way and the judicial tradition of treating the as individuals. In court papers and interviews, the story emerges of one judge struggling with increasing limits on his power to judge. *New York Times* article, by Benjamin Weiser, January 13, 2004. See NYTimes.com for full text of article.

2. The "Feeney Amendment" and Departures

U.S. District Courts have routinely reached differing conclusions about the constitutionality of the so-called "Feeney Amendment" to the Prosecutorial Remedies and the Other Tools to end the Exploitation of children Today Act (Pub. L. No. 108-21). The U.S. District Court for the Central District of California held that the statute's requirement of reports on individual judges who grant downward departures from the U.S. Sentencing Guidelines "chills and stifles judicial independence to the extent that it is constitutionally prohibited." On the other hand, both the California court and a district court in Hawaii agree that other provisions of the Feeney Amendment are permissible extensions of the 1984 Sentencing Reform Act, which was upheld against separation-of-powers challenges in *Mistretta v. United States*, 488 U.S. 316 (1989). (*United States v. Mendoza,* C.D. Calif., No. CR 03-730 DT, 1/12/04, and *United States v. Schnepper,* D. Hawaii, No. 02-00062 ACK, 1/13/04.)

The Feeney Amendment was signed into law in April 2003 as Title IV of the PROTECT Act. The Feeney Amendment placed new constraints on judicial discretion to grant downward departures for reasons other than a defendant's substantial assistance to authorities. It also mandates that the Justice Department inform Congress of individual federal judge' decisions to grant non-substantial assistance downward departures. Sections 401(l)(1) and (2) of the PROTECT act require a report by the Justice Department to Congress of any downward departure, other than one for substantial assistance, setting forth the case, facts, the identity of the district court judge, the stated reason for departure, and parties' position with respect to the departure. Section 401(l)(3) authorized the Justice Department to promulgate its own policies and procedures for reporting to Congress.

Pursuant to Section 401(l)(3), then-Attorney General John Ashcroft sent a report to Congress that included a memorandum dated July 28, 2003, which modified the U.S. Attorney's Manual to require prosecutors to report to the Department of Justice certain categories of downward sentencing departures.

In his recent annual report on the judiciary, Chief Justice William H. Rehnquist was sharply critical of the decision by Congress and the Justice department to collect judge-specific information about downward departure sentences.

3. 5K2.0 Departures

5K2.0(b) provides as follows:

(b) DOWNWARD DEPARTURES IN CHILD CRIMES AND SEXUAL OFFENSES. – Under 18 U.S.C. § 3553(b)(2)(A)(ii), the sentencing court may impose a sentence below the range established by the applicable guidelines only if the court finds that there exists a mitigating circumstance of a kind, or to a degree, that –

(i) has been affirmatively and specifically identified as a permissible ground of downward departure in the sentencing guidelines or policy statements issued under section 994(a) of Title 28, United States Code, taking account of any amendments to such sentencing guidelines or policy statement by act of Congress;

(ii) has not adequately been taken into consideration by the Sentencing Commission in formulating the guidelines; and

(iii) should result in a sentence different from that described.

The grounds enumerated in Part K of Chapter Five are the sole grounds that have been affirmatively and specifically identified as a permissible ground of "downward departure" in these sentencing guidelines and policy statements. Thus, notwithstanding any other reference to authority to depart downward elsewhere in this Sentencing Manual, no other grounds of downward departure are permissible for offenses referred to in this provision.

(Note the broad coverage of the term from the commentary.)

(A). Definition. – For purposes of this policy statement, the 'child crimes and sexual offenses' means offenses under any of the following: 18 U.S.C. § 1201 (involving a minor victim), 18 U.S.C. § 1591, or chapter 71, 109A, 110, or 117 of Title 118, United States Code.

(B). Standard for Departure. –

(i) Requirement of Affirmative and Specific Identification of Departure Ground. – The standard for a downward departure in child crimes and sexual offenses differs from the standard for other departures under this policy statement in that it includes a requirement, set forth in 18 U.S.C. § 3553(b)(2)(A)(ii)(I) and subsection (b)(1) of this guideline, that any mitigating circumstance that forms the basis for such a downward departure be affirmatively and specifically identified as a ground for downward departure in this part (*i.e.*, *Chapter Five, Part K*).

In addition, 5K2.22 provides:

4. §5K2.22. Specific Offender Characteristics as Grounds for Downward Departure in Child Crimes and Sexual Offenses (Policy Statement)

In sentencing a defendant convicted of an offense involving a minor victim under section 1201, an offense under section 1591, or an offense under chapter 71, 109A, 110, or 117, of title 18, United States Code:

(1) Age may be a reason to impose a sentence below the applicable guideline range only if and to the extent permitted by § 5H1.1.

(2) An extraordinary physical impairment may be a reason to impose a sentence below the applicable guideline range only if and to the extent permitted by §5H1.4.

(3) Drug, alcohol, or gambling dependence or abuse is not a reason for imposing a sentence below the guidelines.

5. Booker/Fanfan Decided: A New Era in Federal Sentencing finds Home in Child Pornography Cases

The U.S. Supreme Court decided the consolidated case of United State v. Booker and United States v. Fanfan, on January 12, 2005. This landmark decision will usher in a new era in federal sentencing practice and provides new opportunities in sentencing advocacy. The majority decision is in two parts. The first part, written by Justice Stevens for a 5-4 majority, finds the Guidelines violate the Sixth Amendment and are thus unconstitutional. The second part, written by Justice Breyer for a different5-4 majority, remedies this finding by making the Guidelines advisory, mandating that the courts must consider the Guidelines (among other traditional factors) when rendering a sentence, and finding that appellate courts can review sentences for "reasonableness." The full opinion can be accessed at the Supreme Court's website at www.supremecourtus.gov/opinions/04pdf/04-104.pdf. Below are highlights of the decision:

First Holding: Current Administration of the Guidelines Violates Defendant's Sixth Amendment Rights

Pursuant to 18 U.S.C. Section 3553(b) the Guidelines are mandatory, and thus create a statutory maximum for purpose of Apprendi v. New Jersey, 530 U.S. 466 (2000). The Court applied the reasoning in Blakely v. Washington, and finds that "any fact (other than a prior conviction) which is necessary to support a sentence exceeding the maximum authorized by the facts established by a plea of guilty or a jury verdict must be admitted by the defendant or proved to a jury beyond a reasonable doubt." Under the current administration of the Guidelines, judges find these facts, and thus they are unconstitutional.

Second Holding: The Guidelines are Advisory and Sentences are Reviewable for "Unreasonableness"

Given the Court's first holding, the Court "excises" 18 U.S.C. §3553 (b)(1) and section 3742 (e) from the Sentencing Reform Act and declares the Guidelines are now 'advisory." Pursuant to section 3553 (a), district judges need only to "consider" the Guideline range as one of many factors, including "the need for the sentence ... to provide just punishment for the offense § 3553(a)(2)(A), to afford adequate deterrence to criminal conduct § 3553(a)(2)(B), to protect the public from the further crimes of the defendant § 3553(a)(2)(c). The Sentencing Reform Act, absent the mandate of § 3553 (b)(1), authorizes the judge to apply his own perceptions of just punishment, deterrence, and protection of the public even when these differ from the perceptions of the U.S. Sentencing Commission. The Sentencing Reform Act continues to provide for appeals from sentencing decisions (irrespective of whether the trial judge sentences within or outside the Guidelines range) based on an "unreasonableness" standard.

6. Recent Sentencing Trends: Stabenow, Grober, Dorvee, et al.

Over time, support for the rote application of the Sentencing Guidelines has begun to dwindle to the point that many districts across the Country now have what approaches an actual application of 18 U.S.C. §3553(a). Legal scholars, among them judges, litigators, prosecutors and defense attorneys alike, have begun to peel back the layers of the onion so to speak, to unearth the methods by which the Sentencing Guidelines were arrived at as well as to become committed to proper application of the 18 U.S.C. 3553(a) factors in effort to tease apart the worst offenders from those whose facts and circumstances mitigate against the harsh and sometime callous way the Sentencing Guidelines are applied across the board.

In his nationally recognized article, *"Deconstructing the Myth of Careful Study: A Primer on the Flawed Progression of the Child Pornography Guidelines"* July 2009, Troy Stabenow, Assistant Federal Defender for the Western District of Missouri, analyzed the history and metamorphosis of the Child Pornography Guideline in an effort to provide valuable information in understanding how we got the Guideline we have today for cases involving child pornography.

Stabenow's paper supports the proposition that child pornography Guidelines fail in their purpose of creating a range of penalty reflective of their stated objectives. In short, they were not arrived at using the "an empirical approach based on data about past practices" as

referred to in *Kimbrough v. United States*, 128 S. Ct. 558, 567 (2007).

Stabenow contends that the drastic and ever increasing penalties for child pornography offenders was not the product of an empirically demonstrated need for consistently tougher sentencing. Instead, his reveals that the upward changes were largely the consequence of numerous "morality earmarks" that were slipped into larger bills over the last fifteen years, often without notice, debate, or empirical study of any kind. *Stabenow at p. 3.* The research went so far as to uncover Congressionally mandated changes that actually prevented the Commission from implementing carefully considered modifications which would have actually *lowered* applicable offense levels. *Id*

The harsh child pornography Guidelines were at first formulated with the worst of offenders in mind and, over time, they were expanded to every other class of offender, without regard to research or data which reflected its propriety.

The questions raised by the **Stabenow** paper have begun to filter through the judiciary as well. In *U.S. v. Phinney*, 599 F. Supp. 1037 (E.D. Wis. 2009), Judge Lynn Adelman defended the decision to impose a sentence below guideline range. While the facts of the individual case were necessarily considered, as well as the 18 U.S.C. 3553(a) factors, the court also cited the ***Stabenow*** paper and found that:

> "Judges across the Country have recognized, the guideline for child pornography offenses is seriously flawed and is accordingly entitled to little respect. In this decision, I focus in particular on the guideline as it applies to offenders like the defendant Phinney, those convicted of simply possession."
>
> - ***Phinney*** at 1041

The *Phinney* court opined that **"this [child pornography] guideline is just as flawed as the crack guideline"**, *id.* at 1040. For the *Phinney* court, it decided to follow the guidelines as they had been enacted by the Sentencing commission *before* there was congressional meddling into the issue. *Phinney* at p1041. In *U.S. v. Cruikshank*, 667 F. Supp. 2d 697 (S.D. W. Va. 2009), the court noted the flaws in the formulation of the Sentencing Guidelines and discounted their creation. The *Cruikshank* Court expressed her displeasure of the child pornography Guideline,

> "Because they are not based on empirical data and past practices, the Guidelines for consumers of computer-based child pornography are skewed upward."
>
> **- *Cruikshank*** at 702

The Cruikshank Court discussed some of the flaws such as the incongruence of any assumption that the number of images factors in and somehow presupposes that someone is more likely to be a danger to a child simply by virtue of the fact that they collect images. *Cruikshank* at 700-02.

Slowly, Courts of Appeals have upheld sentences which fall outside and below the Guidelines.

The 5th Circuit has upheld probation for child porn case where guideline range was 46-57 months. The Defendant plead guilty to possession of child porn and the Guideline range was 46-57 months. Court gave 60 months probation. Govt appealed. 5th circuit then reversed and vacated the prob sentence under *US v Duhon*, 440 F,3d 711 (5th Cir. 2006).

The US Supreme Court vacated and remanded under Gall. The Fifth Circuit then affirmed the district court sentence of probation, finding no significant procedural error in the imposition of a non U.S.S.G. sentence. The district court had properly and meticulously considered the section 3553(a) factors. **US v. Rowan**, June 9, 2008, No.05-30536

Even more recently, on December 31, 2012, U.S. District Judge Richard Hinojosa (yes, *that*, Richard Hinojosa) in **U.S. v. Saenz**, (Cause #7:05-cr-00877, Southern District of Texas) followed the notion of individual justice in meting out a 5 year probated sentence to a 25 year old man with no criminal record whose conduct never rose to the level of contact or harm to any child apart from those in the images. The facts and circumstances so moved the Court that a variance from the Guidelines was found to be not only warranted, but in fact, appropriate under the facts of the case before him. *United States v. Dorvee*, 616 F.3d 174, (2d Cir.2010), is an outstanding Second Circuit case that continues down the path

of *United States v. Grober*, 624 F.3d 592 (3d Cir. 2010). Grober presents an outstanding articulation of the conundrum often faced by Defendants in Child Pornography cases.

On the one hand, there are powerful equitable factors which are given no apparent voice by either the Federal Sentencing Guidelines or, for that matter, the practical application of the principles articulated in *Kimbrough* and *Gall*. The District Court issued a well-reasoned opinion which employed a thoughtful analysis of the statutes, Sentencing Guidelines, and case law, in an effort to achieve that pesky concept which, in these cases, usually appears only in apparition form - Justice.

Hint - The District Court, in its 32-page opinion, navigated through the statutes [and the attendant mandatory minimums], Guidelines, and case law, to assess a 60-month sentence against a first time offender whose guideline range was 235-293 months with a statutory maximum of 240 months in Federal Prison.

If you read no other case on this issue beyond *Grober*, you will nevertheless be well-served.

As a result, it is important to know the application of the Federal Sentencing Guidelines on Child Pornography cases as much for their flaws and imperfections in their creation as it is for their impact on those charged with crimes involving child pornography.

In follow up to his 2009 work, Stabenow authored his view of the next step in the process, reforming the guidelines. See *A Method for Careful Study: A Proposal for Reforming the Child Pornography Guidelines* . (Federal Sentencing Reporter, Vol. 24, No. 2, Federal Child Pornography Sentencing (December 2011), pp. 108-136) available at

http://www.jstor.org/stable/10.1525/fsr.2011.24.2.108?origin=JSTOR-pdf

This authoritative work, rife with facts and a smattering of editorial, provides the best framework yet seen by the authors for creating a sentencing scheme that makes sense for this difficult offense.

7. U.S.S.G § 2G2.2

The U.S. Sentencing Commission Guideline for a violation of 18 U.S.C. § 2252(a)(4) was U.S.S.G §2G2.4, until it was repealed on November 1, 2004 by virtue of its consolidation into U.S.S.G. 2G2.2. Now 2G2.2 covers the widest range of child pornography violations.

U.S.S.G 2G2.2. Trafficking in Material Involving the Sexual Exploitation of a Minor; Receiving, Trans -porting, Shipping, Soliciting, or Advertising Material Involving the Sexual Exploitation of a Minor; Possessing Material Involving the Sexual Exploitation of a Minor with Intent to Traffic; Possessing Material Involving the Sexual Exploitation of a Minor

(a) Base Offense Level :

(1) **18**, if the defendant is convicted of 18 U.S.C. § 1466A(b), § 2252(a)(4), or § 2252A(a)(5).

(2) **22**, otherwise.

(b) Specific Offense Characteristics

(1) If (A) subsection (a)(2) applies; (B) the defendant's conduct was limited to the receipt or soli - citation of material involving the sexual exploitation of a minor; and (c) the defendant did not intend to traffic in, or distribute, such material, decrease by 2 levels.

(2) If the material involved a prepubescent minor or a minor who had not attained the age of 12 years, increase by **2** levels.

(3) (Apply the greatest) If the offense involved:

(A) Distribution for pecuniary gain, increase by the number of levels from the table in §2B1.1 (Theft, Property Destruction, and Fraud) corresponding to the retail value of the material, but by not less than **5** levels.

(B) Distribution for the receipt, or expectation of receipt, of a thing of value, but not for pecuniary gain, increase by 5 levels.

(C) Distribution to a minor, increase by **5** levels.

(D) Distribution to a minor that was intended to persuade, induce, entice, or coerce the minor to engage in any illegal activity covered under sub -division (E), increase by **6** levels.

(E) Distribution to a minor that was intended to persuade, induce, entice, coerce, or facilitate the travel of, the minor to engage in prohibited sexual conduct, increase by **7** levels.

(F) Distribution other than distribution described in subdivisions (A) through (E), increase by **2** levels.

(4) If the offense involved material that portrays sadistic or masochistic conduct or other depictions of violence, increase by **4** levels.

(5) If the defendant engaged in a pattern of activity involving the sexual abuse or exploitation of a minor, increase by **5** levels.

(6) If the offense involved the use of a computer or an interactive computer service for the possession, transmission, receipt, or distribution of the material, increase by **2** levels.

(7) If the offense involved—

(A) at least 10 images, but fewer than 150, increase by **2** levels;

(B) at least 150 images, but fewer than 300, increase by **3** levels;

(c) at least 300 images, but fewer than 600, increase by **4** levels; and

(D) 600 or more images, increase by **5** levels.

(c) Cross Reference

(1) If the offense involved causing, transporting, permitting, or offering or seeking by notice or advertisement, a minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of such conduct, apply §2G2.1 (Sexually Exploiting a Minor by Production of Sexually Explicit Visual or Printed Material; Custodian Permitting Minor to Engage in Sexually Explicit Conduct; Advertisement for Minors to Engage in Production), if the resulting offense level is greater than that determined above.

8. Computer Enhancement: U.S.S.G § 2G2.2(b)(6) [+2]

Note: Under the revised sentencing guidelines, a defendant will receive a two-offense-level enhancement "if the offense involved the use of a computer." U.S.S.G. § 2G2.2 (b)(6). Defendant contended 2G2.2(b)(3) applied only where the possessor sent images via a computer, not when the possessor merely received; HELD: affirmed; enhancement applies whenever images are transported over the Internet. U.S. v. Johnson, 183 F.3d 1175 (10th Cir. 1999).

Defendant's use of computer in relation to charge of receipt of child pornography in interstate commerce, later dismissed, did not warrant base-offense-level enhancement for offense of smuggling child pornography into the United States, for which defendant was convicted; Sentencing Guidelines' enhancement for use of computer applied only to offense of conviction, not to purportedly attendant relevant conduct. 2G2.2(b)(3), United States v. Boudreau, 250 F.3d 279 (5th Cir. 2001).

The U.S. Court of Appeals for the Fourth Circuit held on March 28, 2003 that an undercover law enforcement officer's use of a computer to send an advertisement for child pornography to a defendant served as a sufficient basis for the enhancement provided by Section 2G2.2(b)(5) of the U.S. Sentencing Guidelines ("[i]f a computer was used for the transmission of the material or a notice or advertisement of the material.").

A postal inspector posted an advertisement for videotapes featuring child pornography on an Internet newsgroup. The defendant ordered some of the tapes. When the tapes arrived by mail, the defendant was arrested and convicted of possession of child pornography. The court agreed with the Seventh Circuit in *United States v. Richardson*, 238 F.3d 837 (7th Cir. 2001), that the enhancement is based on the added dangerousness arising from the anonymity provided by the Internet and that this anonymity

blankets receivers of ads as well as senders.

9. Prepubescent Minor or Minor Children Under Age 12: U.S.S.G § 2G2.2(b)(2) [+2]

The two-level enhancement applicable to receipt of sexually explicit material involving prepubescent minors and minors under age 12 cannot be applied to a defendant who did not intend to receive material involving prepubescent children or children under age 12. United States v. Saylor, 959 F.2d 198 (11th Cir. 1992). Evidence sufficient to support a two-level increase under 2G2.2(b)(1)); United States v. Kimbrough, 69 F.3d 723 (5th Cir. 1995). See United States v. Cole, 61 F.3d 24 (11th Cir. 1995)(insufficient evidence of child pornography depicting minors under twelve).

Sentence for knowing receipt of child pornography was properly enhanced under Sentencing Guidelines on basis of knowing receipt of materials involving prepubescent minor upon court's determination that at least one of the images depicted child under age of 12, and possibly as young as six or seven, and defendant's reckless disregard for ages of subjects. United States v. Fox, 248 F.2d 394 (5th Cir. 2001).

10. Distribution Enhancement: U.S.S.G § 2G2.2(b)(3)(F) [+2]

The Fifth Circuit says that purely gratuitous "distribution" of child pornography justifies five-level increase. The circuits are split on whether the term "distribution" in § 2G2.2(b) includes purely gratuitous dissemination of child pornography. The Eighth Circuit in United States v. Imgrund, 208 F.3d 1070, 1072 (8th Cir. 2000) held that purely gratuitous dissemination does not trigger the five-level increase. The Seventh and Ninth Circuits agree with the Eighth Circuit. United States v. Laney, 189 F.35 954 (9th Cir. 1999), United States v. Black, 116 F.3d 198 (7th Cir. 1997). However, the Second and Eleventh Circuits disagree. See United States v. Lorge,166 F.3d 516, 518 (2d. Cir. 1999) and United States v. Probel, 214 F.3d 1285, 1288 (11th Cir. 2000). The Fifth Circuit agreed with the Second and the Eleventh Circuits holding that a plain reading of the term "distribution" in § 2G2.2(b)(2) includes purely gratuitous distribution of child pornography. Defendant's sentence was affirmed. United States v. Hill, 258 F.3d 355 (5th Cir. 2001), United States v. Simmonds, 262 F.3d 468 (5th Cir. 2001).

Application of sentencing guidelines offense level increase when sentencing defendant for distributing child pornography, on the ground that the offense involved the "distribution" of child pornography, was proper, even if defendant was not paid for any of the pornographic images that he sent to others over the Internet, since "distribution," as used in sentencing guideline, was not limited to transactions entered into for pecuniary gain, but included defendant's "trading" of pornographic images. U.S.S.G § 2G2.2(b)(2), 18 U.S.C.A. United States v. Lyckman, 235 F.3d 234 (5th Cir. 2000).

Defendant's distribution of child pornography with the purpose of enticing a minor to have sex with him warrants the five-level distribution enhancement. United States v. Canada, 110 F.3d 260 (5th Cir.). Also see United States v. Fowler, 216 F.3d 459 (5th Cir. 2000). Compare United States v. Black, 116 F.3d 198 (7th Cir. 1997) (enhancement under 2G2.2 (b)(2) not available unless the distribution is for pecuniary gain); United States v. Delmarle, 99 F.3d 80 (2d Cir. 1996) (departure under 5K2.0 warranted for computer transmission of images used to solicit sexual activity with a minor).

In calculating the fair market value of child pornography, the government may take a defendant's own figures for recent sales and current catalogue offerings and apply them to the defendant's existing inventory, including retail value of the tapes to be reproduced from master tapes. United States v. Kemmish, 120 F.3d 937 (9th Cir. 1997). See also United States v. Stanton, 973 F.2d 608 (8th Cir. 1992).

11. Sadistic or Masochistic Portrayal Enhancement: U.S.S.G § 2G2.2(b)(4) [+4]

When a pornographic image depicts sexual/physical penetration of young child by an adult male, the conduct portrayed is sufficiently painful, coercive, abusive, and degrading to qualify as "sadistic or violent" within the meaning of sentencing guideline providing for four level offense level increase for offense involving material portraying sadistic or masochistic conduct or other depictions of violence. U.S.S.G

§ 2G2.2(b)(3), 18 U.S.C.A. United States v. Lyckman, 235 F.3d at 235.

The Fifth Circuit held that possession of sadistic pictures was not relevant conduct to sending pornography. Defendant sent child pornography via the Internet to "Katrina," an undercover agent. Police recovered from his residence several electronic images of sadistic sexual conduct, two of them depicting minors. The Fifth Circuit reversed a § 2G2.2(b)(3) increase for sadistic material, holding that defendant's receipt and possession of the sadistic pictures was not relevant conduct to his transmission of child pornography. The electronic mailing occurred at a discrete moment, and defendant's receipt of the other, sadistic images did not occur "during the commission of the offense of conviction." United States v. Fowler, 216 F.3d 459 (5th Cir. 2000).

Defendant's trafficking in material portraying sadistic conduct -- anal and vaginal penetration of minors through the use of sexual devices -- warranted a four-level enhancement under U.S.S.G. § 2G2.2(b)(3). United States v. Canada, 110 F.3d 260 (5th Cir. 1997).

A photograph depicting a nude minor boy having an unidentified object inserted into his anus constituted a sadistic portrayal warranting a four-level enhancement. United States v. Delmarle, 99 F.3d 80 (2d Cir.1996). Enhancement also found to be proper in United States v. Garrett, 190 F.3d 1220 (11th Cir. 1999).

Defendant's possession of pornographic magazines depicting minors engaged in sadomasochism constituted "relevant conduct" that could be considered under § 2G2.2(b)(3). United States v. Ellison, 113 F.3d 77 (7th Cir. 1997).

United States v. Kimbrough, 69 F.3d 723 (5th Cir. 1995). Two images that depicted female minor in bondage out of hundreds was sufficient to support four-level enhancement for possessing material portraying sadistic or masochistic conduct.

Logs of Internet conversations can support this enhancement, United States v. Tucker, 136 F.3d 763 (11th Cir. 1998) (scienter is an element of this enhancement).

United States v. Richardson, 238 F.3d 837 (7th Cir. 2001). Section 2G2.2(b)(3) is imposed on the basis of strict liability. Defendant who possessed 77 images of bondage and torture downloaded in bulk from sources that didn't indicate the range of sexual practices depicted, assumed a substantial risk of receiving such images, so enhancement applied.

United States v. Parker, 267 F.3d 839 (8th Cir. 2001). Image files of adult males standing over and urinating in the face of a female child, adult male ejaculating into the face and open mouth of a crying baby, sexual penetration of a minor girl using a large carrot were depiction of violence or sadism warranting the four-level increase in § 2G2.2(b)(3).

United States v. Dunlop, 279 F.3d 965 (11th Cir. 2002). Although photos of sadistic conduct did not form the basis of defendant's conviction, defendant's possession of the images when he transmitted other images of child pornography warranted sentence enhancement under 2G2.2(b)(3).

12. Pattern of Sexual Exploitation: U.S.S.G § 2G2.2(b)(5) [+5]

Five-level enhancement for a pattern of sexual exploitation of minors does not apply to traffickers who are not directly involved in the actual abuse or exploitation of minors. United States v. Kemmish, 120 F.3d 937 (9th Cir. 1997); see also United States v. Neilssen, 136 F.3d 965 (4th Cir. 1998) (however, enhancement may apply to unrelated sexually abusive conduct of minors). Computer transmission of child pornography is not sexual exploitation of minor. United States v. Chapman, 60 F.3d 894 (1st Cir. 1995). United States v. Ketcham, 80 F.3d 789 (3d Cir. 1996), enhancement for exploitation of a minor was reversed in a child pornography case for insufficient evidence. United States v. Anderton, 136 F.3d 747 (11th Cir. 1998) (exploitation does not have to be part of the offense of conviction).

Defendant's four prior convictions of obscene phone calls to young girls and prior felony conviction for indecent exposure to children inadequate for this enhancement. United States v. Pharis, 176 F.3d 434 (8th Cir. 1999).

Evidence that defendant had been convicted 20 years earlier of two counts of rape and two counts of posing or exhibiting a child, and had sexually abused between twelve and fifteen children in his neighborhood during four-year period of conduct prior to his conviction, was sufficient to establish pattern of activity involving sexual abuse of exploitation of a minor that would

warrant an increase in his base offense level under the Sentencing Guidelines following his convictions on child pornography and weapons charges. United States v. Woodward, 277 F.3d 87 (1st Cir. 2002).

United States v. Lovaas, 241 F.3d 900 (7th Cir. 2001). The conduct considered for purposes of the "pattern of activity" enhancement is broader than the scope of relevant conduct typically considered under § 1B1.3. Decades-old instances of sexual misconduct were properly relied upon by court as basis for § 2G2.2(b)(4) enhancement.

United States v. Polson, 285 F.3d 563 (7th Cir. 2002). Five-level enhancement under § 2G2.2(b)(4) affirmed despite fact that evidence of one of the prior incidents consisted of multiple hearsay.

United States v. Woodward, 277 F.3d 87 (1st Cir. 2002). Five-level enhancement affirmed even though def. had only one prior conviction. Judge can consider all conduct proven by a preponderance of the evidence, whether or not the incident in question resulted in a conviction.

United States v. Ashley, 342 F.3d 850 (8th Cir. 2003). Five-level enhancement affirmed where defendant had a 5 year-old conviction for 2 counts of gross sexual imposition for molesting his son and daughter.

United States v. Gunderson, 345 F.3d 471 (7th Cir. 2003). Court affirmed five-level enhancement even though the relevant prior conviction was for consensual sex with a 16-year-old when the defendant was twenty-two years old.

13. Minor Role Adjustment: U.S.S.G § 3B1.2

No minor role adjustment warranted based on defendant's claim "that he was simply one of a large network of people engaged in the exchange of child pornography through computers and therefore played a minuscule role in a grandiose pornography operation: via a Danish bulletin board service ("BBS"). United States v. Everett, 129 F.3d 1222, 1224 (11th Cir. 1997).

14. Use of Minor to Commit Crime: U.S.S.G § 3B1.4

Two-level adjustment for use or attempt to use a person less than eighteen years of age to commit the offense or assist in avoiding detection of, or apprehension for, the offense. The government sought use of minor enhancement and pattern of sexual activity in United States v. Pharis, 176 F.3d 434 (8th Cir. 1999), but the court refused to apply either. Mr. Pharis used the Internet to communicate with a 13 year-old girl who was really an agent and sent pornographic images. The court held that a victim must be under age of 18 for "use of minor" enhancement under § 3B1.4; rule of lenity gives reading of guideline to defendant who believed he was communicating with a 13 year old girl who in fact was two law enforcement officials cannot be enhanced with this section based on the rule of lenity.

15. Grouping: U.S.S.G § 3D1.2

The "victims" under § 3D1.2 (b) of the distribution of child pornography are the children depicted in the illegal material, rather than society as a whole, and thus substantive counts involving pictures of different minors should not be grouped for purposes of sentencing. United States v. Boos, 127 F.3d 1207 (9th Cir. 1997).

The defendant was not entitled to have counts grouped for sentencing, as multiple children depicted in multiple pornographic images could be treated as different victims for sentencing purposes. United States v. Norris, 159 F.3d 926 (5th Cir. 1998); and United States v. Ketchum, 80 F.3d 789 (3d Cir. 1996).

Alert: See "new" U.S.S.G amendment for "closely related counts" effective November 1, 2001. The amendment resolves the split of authority between Norris and Toler.

The 2001 amendments clarify that multiple counts involving different children are to be grouped. U.S.S.G § 3D1.2(d) (Nov. 1, 2001). The Fifth Circuit has held that this amendment was a substantive change that cannot be applied retroactively. United States v. Davidson, 283 F.3d 681 (5th Cir. 2002). Because exploitation is a specific offense characteristic, however, conviction for this offense is grouped with possession and receipt of child pornography. United States v. Runyon, 290 F.3d 223 (5th Cir. 2002).

16. Ten or More: U.S.S.G § 2G2.4(b)(2) REPEALED

Under the previous Guideline, there was

a 2 level upward adjustment for possession of "ten or more books, magazines, periodicals, films, video tapes, or other *items*, containing a visual depiction involving the sexual exploitation of a minor." With the advent of 2G2.2, this adjustment has been subsumed in the myriad of other methods of heightening a sentence called for by that guideline.

17. Diminished Capacity Departure: U.S.S.G § 5K2.13

The Third Circuit in United States v. McBroom, 124 F.3d 533, 548 (3d Cir. 1997) mandated that in considering a diminished capacity defense, the court must consider not only a defendant's cognitive capacity, but also his volitional capacity. Following that, the district court departed downward based on the defendant's obsessive/compulsive disorder that caused him to view Internet porn even though he knew he would soon be caught by the FBI. United States v. McBroom, 124 F.3d 533 (D.N.J. 1998); *cf*. United States v. Miller, 146 F.3d 1281 (11th Cir. 1998) (defendant's impulse control disorder did not contribute to his transport of child pornography through the computer). Note: See Feeney Amendment and the "new" 5K2.0.

A defendant's diminished capacity, in the form of an obsessive-compulsive disorder that allegedly compelled him to gather child pornography over the internet even though he knew it was wrongful, and even though he had previously provided his online user names and passwords to police and knew that they were virtually certain to discover his continued activity, was a legally permissible basis for a downward sentencing departure. It was a factor not taken into account by the Sentencing Commission in formulating the guideline applicable to the defendant's offense. United States v. Lighthall, 389 F.3d 791 (8th Cir. 2004).

Defendant convicted on a guilty plea to receiving and distributing computer files that contained child pornography would be granted a downward sentencing departure on the basis of diminished capacity; his involvement in child pornography was not a product of controlled rational calculation, but rather, stemmed from a pornographic obsession in constant need of fueling; this obsession escalated to the point where he spend hours collecting and transmitting thousands of pornographic images indiscriminately, becoming hyper-aroused by almost anything and desensitized to child pornography. Unites States v. Tanasi, 2004 WL 406724 (S.D.N.Y 2004).

18. Post-Offense Rehabilitation

Two-levels downward departure warranted based on defendant's extraordinary post-offense rehabilitation efforts -- daily attendance at AA, continued sobriety, weekly attendance at therapy sessions, compliance with medication, full-time employment, and commitment to family responsibilities. United States v. McBroom, 124 F.3d 533 (D.N.J. 1998); see also United States v. Kapitzke, 130 F.3d 820 (8th Cir. 1997); United States v. Shasky, 939 F. Supp. 695 (D. Neb. 1996). Note: See Feeney Amendment and the "new" 5K2.0.

19. Susceptibility to Abuse

A downward departure for susceptibility to abuse in prison is only warranted in extraordinary cases, not in a case where the defendant is of average size and good health. United States v Drew, 131 F.3d 1269 (8th Cir. 1997); United States v. Kapitzke, 130 F.3d 820 (8th Cir. 1997). Compare United States v. Wilke, 995 F.Supp. 828 (N.D. Ill. 1998) (defendant unusually susceptible due to his sexual orientation and his passive, meek demeanor); United States v. Shasky, 939 F. Supp. 695 (D. Neb. 1996). Note: See Feeney Amendment and the "new" 5K2.0.

20. Possession v. Distribution - Is there a Guideline difference?

Often a Defendant who was caught using his computer to receive and ultimately distribute such illegal material can win a portion of the battle if he is allowed to enter a plea of "guilty" to "Possession" instead of "Distribution" of the materials involving the sexual exploitation of a minor.

The thinking is that the Defendant will have a net savings of 2 levels [§2G2.2 (a)(1) is an 18 + the §2G2.2(b)(6) use of a computer enhancement = 20] versus the starting place of §2G2.2(a)(2) base offense level 22.

However, note that this savings might also be achieved if a prosecutor requires a plea to the

more onerous "Distribution" when a Defendant can show the facts in support of application of §2G2.2(b)(1) which provides for a 2 level decrease from 22 if the Defendant's conduct was limited to receipt or solicitation and the defendant did not intend to traffic in, or distribute, such material.

K. Child Pornography Restitution Title 18 U.S.C. §2259

18 U.S.C. §2259 provides that a District Court "shall order restitution" directing a Defendant to pay to a victim(s), the "full amount of the victim's losses" as determined by the Court.

The statutory definition of "victim" includes a child whose image was used in the production of child pornography. This statute has become a "hotbed" issue of late and the effects of its application have yet to be fully developed.

What constitutes "victim's losses" is expansive under §2259(b)(3) and includes:

(A) medical services relating to physical, psychiatric, or psychological care;

(B) physical and occupational therapy or rehabilitation;

(C) necessary transportation, temporary housing, and child care expenses;

(D) lost income;

(E) attorneys' fees, as well as other costs incurred; and

(F) any other losses suffered by the victim as a proximate result of the offense.

§2259 has been used by several of the children (now adults) to secure enormous judgments against defendants convicted of child-pornography-related offenses - some of which are in the millions of dollars.

Note: The statute, as written, seems to have an embedded requirement that the losses be those that are "proximately caused" by the actions of the defendant and many district courts are requiring such a showing before the imposition of any monetary restitution order against those convicted of child-pornography-related offenses. The "causation" requirement appears to be the battleground upon which the fight against such crippling restitution orders can be successfully waged.

Various Circuit Courts of Appeals had dealt with this issue, including the 1st, 2nd, 4th,5th, 6th,9th, and 11th. All but the 5th generally support the notion that causation by a particular Defendant be required prior to entry of a restitution Order can be entered. The 5th Circuit dealt with the issue in *Paroline*, wherein it reversed the District Court's decision that no restitution should issue when there was insufficient evidence to establish a causal connection between the conduct of the defendant and the victimization of the child. *In Re Amy & U.S. v. Paroline*, 636 F.3d 190 (5th Cir. 2011). The Fifth Circuit ruled that the plain meaning of the statute required no causal link of harm to a victim by a particular Defendant, rather, it merely required proof of harm to the victim alone on account of the images in possession of a Defendant.

The resulting order would look more like an Order imposing joint & several liability and contribution from others against whom and order was entered.

Predictably, this issue centered around causation and how and whether it intersects with the statute was presented to the Supreme Court and was argued on January 22, 2014 and the opinion issued April 23, 2014.

The Supreme Court in *Paroline* held essentially that any interpretation of the statute that would impose a strict liability for full restitution for damages caused to a victim, regardless of the proximate cause by a particular defendant of the damages for which restitution might order, is erroneous.

The Court ordered that the District Court would be required to take evidence on any particular Defendant's role in causing the harm to the victim and that the Government would have the burden of proving the liability of a defendant - by preponderance of the evidence, for the commensurate damages caused by his conduct alone.

In essence, gone are the days where a Defendant could have an order of Restitution entered against him under 18 U.S.C. §2259 without a finding of both (1) "proximate cause" of the Defendant's harm done to the victim and (2) some determination of the how the monetary assessment of restitution against a particular Defendant coincides proportionately with the degree of harm caused by the particular Defendant's conduct.

The full text of the opinion is available at:

http://www.supremecourt.gov/opinions/13pdf/12-8561_7758.pdf

L. Conditions of Supervised Release

District courts have broad discretion to fashion conditions of supervised release. United States v. Edgin, 92 F.3d 1044, 1048 (10th Cir. 1996). The court has authority to order compliance with sex registration requirements for a particular state as a condition of release. United States v. Fabiano, 169 F.3d 1299 (10th Cir. 1999). Under 18 U.S.C. § 3583(d) and § 3553(a)(2), all that is required is that the condition be "reasonably related" to the "nature and circumstances of the offense and the history and characteristics of the defendant, and that the condition involve no greater deprivation of liberty than is reasonably necessary to deter criminal conduct, protect the public, and provide the defendant with needed educational or vocational training, medical care, or other correctional treatment.

The U.S. Court of Appeals for the Seventh and Eighth Circuits released opinions within a day of one another that address restricting convicted felons' use of computers and the Internet as a condition of their release. Both circuits agree that such restrictions are appropriate as long as they are reasonably related to the statutory purposes underlying conditions of release, involve no greater deprivation of liberty than is reasonably necessary, and are not overly broad. While the two decision address convictions for the possession and/or sale of child pornography, the principles they articulate apply to any sentence imposed for using a computer as a criminal instrumentality. *United States v. Holm*, 326 F3.d 872 (7th Cir. 2003) and *United States v. Fields*, 324 F3.d 1025 (8th Cir., 2003).

In a case of first impression in the circuit, the U.S. Court of Appeals for the Eleventh Circuit on February 14, 2003, took its place in a split of authority over banning convicted sex offenders from using the Internet while on supervised release. The court sided with the Fifth and Tenth Circuits in upholding the restriction. *United States v. Zinn*, 321 F.3d 206 (3d Cir. 2003).

The Third Circuit evaluated the sentence of a man in his 60's who was arrested for possessing a large collection of computerized images of child pornography. The court reversed the lower court ban on accessing the Internet as a condition of release. *United States v. Freeman*, 316 F.3d. 686 (3d Cir. 2003).

When a defendant is convicted for transmission of child pornography, the court may order as a condition of supervised release that the community (*i.e.* law enforcement officials, school officials, and neighbors) be notified of the conviction. United States v. Coenen, 135 F.3d 938 (5th Cir. 1998).

Forbidding access to the Internet, BBS, or "exchange format involving computers" is an appropriate condition of supervised release. United States v. Crandon, 173 F.3d 122 (3d Cir. 1999).

In United States v. Sofsky, 287 F.3d 122 (2d Cir. 2002), the court struck a condition of supervised release that "the defendant (who was convicted of possessing child pornography) may not 'access a computer, the Internet, or bulletin board systems at any time, unless approved by the probation officer.'" The Second Circuit vacated the internet restriction because it was broader than reasonably necessary. In doing so, the Court of Appeals relied on its earlier decision in United States v. Peterson, 248 F.3d 79 (2d Cir. 2001).

United States v. Paul, 274 F.3d 155 (5th Cir. 2001) (affirming complete ban on computer or internet use); United States v. White, 244 F.3d 1199 (10th Cir. 2001) (reversing complete ban).

Condition of defendant's probation prohibiting defendant from possessing any pornography was unconstitutionally vague; condition of defendant's probation prohibiting defendant from residing in "close proximity" to places frequented by children was unconstitutionally vague; and condition of defendant's probation, requiring defendant to submit to any search by law enforcement or probation officers was not over broad. United States v. Guagliardo, 278 F.3d 868 (9th Cir. 2002).

Condition of supervised release prohibiting defendant from possessing "all forms of pornography, including legal adult pornography," was unconstitutionally vague; and condition of supervised release prohibiting defendant from having unsupervised contact with minors was supported by evidence. United States v. Loy, 237 F.3d 251 (3d Cir. 2001).

United States v. Angle, 234 F.3d (7th Cir. 2000). Court found that defendant was entitled to notice prior to sentencing of special condition to register as a sex offender. Samples of the images

included in the record supported defendant's guilty plea. There was no support in the record that defendant based his plea on a belief that the images depicted virtual children.

United States v. Deaton, 204 F. Supp.2d 1181 (E.D. Ark. 2002). The court held that a complete ban on Internet use was "overly broad and not reasonably necessary due to the importance of the Internet as a source of information and means of communication. Distinguishing the "egregious conduct of the defendant in Paul, the court modified the sentence of defendant, who was convicted of possession, tp prohibit him from using the Internet without permission from the probation dept.

United States v. Cabot, 325 F.3d 384 (2d Cir. 2003). Court vacated condition that P.O. approve any computer and internet usage by the defendant.

United States v. Knight, 86 Fed. Appx. 2 (5th Cir. 2003). Defendant pled guilty to receipt of cp. The court found that a condition banning use of the internet was not an abuse of the dist ct s discretion.

United States v. Andis, 333 F.3d 886 (8th Cir. 2003). As defendant waived his right to appeal in the plea agreement, he could not appeal his condition of release. The court noted, however, that a right of appeal will remain, despite a plea agreement, for a claim of illegal sentence or miscarriage of justice.

George Washington University Law School Associate Professor Orin S. Kerr, a frequent commentator on cybercrime cases, summarizes the cases as follows: "If a defendant has used the Internet to contact minors, the court can create a flat ban use of the Internet (as in *Sofsksy*), or has merely developed a collection of computerized images through other means (as in *Freeman*), a flat ban is too broad. The trick is too look to whether the defendant has used Internet to contact the victims."

M. Sex Offender Registration

On November 26, 1998, a number of new federal provisions concerning sex offenders became effective. The new laws are complicated.

The new amendments to 18 U.S.C. §§ 3563(a), 3583(d), and 4209(d) require that, as mandatory condition of probation, supervised release, and parole, an offender convicted of any of the federal sex offenses described in 18 U.S.C. § 4202(c)(4) register in any state in which he lives, is employed, carries on a vocation, or is a student.

1. Federal Law

The following offenders must register under the provisions of 18 U.S.C. §§ 3563(a) and 3583(d) as amended.

1. Any offender who committed an offense listed in 18 U.S.C. § 4042(c)(4) on or after November 26, 1998, pursuant to the new mandatory condition that must be imposed under the provisions of §§ 3563(a) and 3583(d).

2. Any offender who committed an offense listed in § 4042(c)(4) prior to November 26, 1998, if the federal conviction for that offense requires registration under state law, pursuant to the §§ 3563(a)(1) and 3583(d) mandatory conditions of release that an offender comply with all federal, state, and local laws.

3. Any other offender who committed an offense that under state law requires registration, pursuant to the §§ 3563(a)(1) and 3583(d) mandatory conditions of release that an offender comply with all federal, state, and local laws. These offenses may include federal offenses not included in § 4042 but covered under the state registration statute, and they may include offenses committed before the enactment of the state registration law if the state law is retroactive.

4. Any offender for whom the court has imposed a special condition of release that requires registration under the provisions of 18 U.S.C. §§ 3563(b)(22) and 3583(d).

Note: Sex Offender Internet Registration Statutes Upheld by High Court in 2003. The U.S. Supreme Court has upheld two states' Megan's Laws in a pair of cases raising individual rights challenges. The Court unanimously held that persons required to register as sex offenders have no procedural due process right to a hearing on whether they are currently dangerous. The Court also held that sex offender registration is not an unconstitutional ex post facto law as applied to registrants who committed sex crimes prior to enactment. *Smith v. Doe*, 538 U.S. 84 (2002), and *Connecticut Dept. of Pub. Safety v. Doe*, 535 U.S. 1077 (2002).

Note: Federal DNA Database law Violates Fourth Amendment? The 2000 DNA Analysis Backlog Elimination Act, 42 U.S.C. § 14135, which requires certain defendants under

federal supervised release to provide DNA samples for inclusion in a federal database, violates the Fourth Amendment as interpreted in *Indianapolis, Ind. v. Edmond*, 531 U.S. 32 (2000), and *Ferguson v. Charleston, S.C.*, 532 U.S. 67 (2001).

The act requires a defendant who "is or has been" convicted of a qualifying felony to provide a DNA sample for the FBI's CODIS database. The defendant in this case is on supervised release following a conviction of a non-qualifying felony, but in 1974, he was convicted of and served a sentence for a crime that does qualify under the act. The probation department petitioned to revoke the defendant's supervised release on the basis of his refusal to submit to DNA testing pursuant to the act. *U.S. v. Kincade*, 345 F.3d 1095 (9th Cir. 2003) held that Act is unconstitutional, but the 9th Circuit vacated the panel opinion on January 5, 2004, and granted an en banc hearing. *But see*: *Groceman v. U.S. Dept. of Justice*, 354 F.3d 411 (5th Cir. 2004) ruled that Act is constitutional (Plaintiffs were prisoners seeking to enjoin various state agencies from collecting and retaining samples of their DNA pursuant to the ACT. Court held that persons incarcerated after conviction retain no constitutional privacy interest against their correct identification and thus, collection of DNA from prisoners under Act is reasonable under the 4th Amendment). See "Validity, Construction, and Application of DNA Analysis Backlog Elimination Act of 2000, 42 U.S.C.A. §§ 14135 et seq and 10 U.S.C.A. § 1565" 187 A.L.R. Fed. 373, § 3a (2003) HN: 3,4 (F.3d) for a discussion of the issues and cases regarding this Act.

2. Texas State Law

Texas Penal Code § 62.01 does require individuals with federal and military convictions to register.

In 1994, federal legislation directed each state to draft and implement its own sex offender registration law. Some state statutes specifically include federal convictions, others do not. The Texas statute originally referred only to convictions under state law and the UCMJ. No reference or mention was made to federal convictions. The code was amended in 1999.

A sex offender may seek an exemption from registration if he has only a single reportable conviction of adjudication and the court has filed with the court papers an affirmative finding that at the time of the offense, the defendant was younger than 19 years of age and the victim was at least 13 years of age, and the conviction is based solely on the ages of the defendant and the victim or intended victim at the time of the offense. The court may grant the exemption on proof from a registered treatment provider that the exemption does not threaten public safety, and that the conduct was consensual. The exemption is revocable. The procedures are retroactive for adults and juveniles. Tex. Code Crim. Pro. Art. 62.105; 42.017. (HB2987). Sex offenders who get community supervision must give a sample of their DNA to DPS. Tex. Cod Crim. Pro. Ch. 62; art. 42.12. (SB 1380).

3. All 50 States Linked to Department of Justice National Sex Offender Public Registry Website

As of July 2006, all 50 states are now participating in the National Sex Offender Public Registry (NSOPR) Website, the Justice Department announced South Dakota and Oregon have now been added to the Website, which provides real-time access to public sex offender data nationwide with a single Internet search. The Department of Justice sponsored site allows parents and concerned citizens to search existing public state and territory sex offender registries beyond their own states.

X. Educating Yourself and the Judge

Defense counsel must educate the judge on all of these issues. Although computers are now widely used in office settings, the Internet and the field of computer images are not widely understood by those who use them. Many of us use a desktop or laptop computer to perform word processing and the like, but not many understand the process involved. Neither should we expect the trial judge to do so. The attorney should write every motion and use every hearing to educate the judge as to the complexity of the case and what needs to be done. This will take more time than most criminal cases, but is necessary to convince the judge that your case is more than one involving "dirty pictures."

I also recommend that attorneys consult the Department of Justice Federal Guidelines on Searching & Seizing Computers (2002) (DoJ Guidelines). This document is essential reading in any computer crime case. The full text of both the DoJ Guidelines and the DoJ Supplement can be found on DoJ's website, www.usdoj.gov/criminal/cybercrime .

Highly Recommended Computer Forensic Site: International Journal of Digital Evidence, http://www.informatik.uni-trier.de/~LEY/db/journals/ijde/index.html

XI. ACKNOWLEDGMENT AND SOURCES

The following sources, articles, materials, reports, and individuals were utilized in preparing the presentation for this paper, to-wit:

1. Jeffrey M. Flax

   (Former) National Systems Support Analyst

   F.P.D Denver, Colorado

   "Challenges in Defending Clients Accused of Internet Pornography"

2. Kari L. Bourg

   Research and Writing Specialist

   F.P.D Denver, Colorado

   "Challenges in Defending Clients Accused of Internet Pornography"

3. Zig Popko

   A.F.P.D. , District of Arizona

   Phoenix, Arizona

   "Child Pornography and the Internet," "CJA Defense Journal"

4. Jennifer Stewart, "If This is the Global Community, We Must Be on the Bad Side of Town: International Policing of Child Pornography on the Internet," 20 Hous. J. Int'l L. 205, 207 (1997).

5. *Philadelphia Inquirer* newspaper; article dated Friday, June 19, 1998.

6. *Washington Post* newspaper; article dated July 22, 1998.

7. *New York Times* newspaper; article dated July 22, 1998, and January 13, 2004.

8. Samantha Friel, "Porn by Any Other Name? A Constitutional Alternative to Regulating 'Victimless' Computer-Generated Child Pornography," 32 Val.U.L.Rev. 207, 1997.

9. Testimony of D. Douglas Rehman before the Congress of the United States, House of Representatives, Committee on the Judiciary Subcommittee on Crime, on October 7, 1997.

10. Materials obtained from the Naval Justice School, Newport, Rhode Island.

11. Kristi Wilmoth

    Legal Assistant

    Office of the Federal Public Defender

    110 North College, Suite 1122

    Tyler, Texas 75702

12. Materials prepared by the Office of the SJA, United States Air Force, Office of Special Investigations.

13. Materials and information prepared by the U.S. Department of Justice, Cybercrime Division.

14. *The Third Branch* (a newsletter of the federal courts), "Cybercrime: New Way to Commit Old Crimes."

15. *Denver Post* newspaper; article dated 8/9/2001.

16. Public Access to Court Electronic Records (PACER), provided by the Administrative Office of the United States Courts.

17. Practicing Guide for Defending a Federal Criminal Case, www.fdewi.org, 2001 Ed.Steve Campbell

    Computer Systems Administrator

    Federal Public Defender for D.C.

    625 Indiana Ave. NW, Suite 550

    Washington, DC 20004

    202-208-7500 x119

    steve_campbell@fd.org, www.dcfpd.org