

A Year In Review:

Precedents in Computer and Internet

Security Law

2005-2006

**DEFCON 14
August 4, 2006
Major R.W. Clark
U.S. Army, JAGC**

Agenda

- **Issues in Computer & Internet Security**
- **Computer & Internet Legal Precedents August 2005 to July 2006**
- **Computer Crime Prosecutions, Arrests & Indictments August 2005 to July 2006**

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.*

My Background



Robert Clark

No relationship to Richard Clarke

Legal Issues 2005-2006



Legal Issues 2005-2006

The President shall be Commander in Chief of the Army and Navy of the United States, and of the Militia of the several States, when called into the actual Service of the United States.

U.S. CONST. Art. II, § 2, cl. 1

The Congress shall have Power to . . . Provide for the common Defence and general Welfare of the United States;

To provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrections and repel Invasions;

U.S. CONST. Art. I, § 8

Legal Issues 2005-2006

Interpretations of Conflicting Constitutional Sections

1. The power of the President is at its zenith under the Constitution when the President is directing military operations of the armed forces, because the power of the Commander in Chief is assigned solely to the President.

Military Operations Against Terrorists and Nations Supporting Them, Op. Off. Legal Counsel (Sept. 25, 2001)

found at <http://www.usdoj.gov/olc/warpowers925.htm>

2. The scope of the President's authority to commit the armed forces to combat is very broad.

Memorandum for Honorable Charles W. Colson, Special Counsel to the President, from William H. Rehnquist, Assistant Attorney General, Office of Legal Counsel, *Re: The President and the War Power: South Vietnam and the Cambodian Sanctuaries* (May 22, 1970)

Legal Issues 2005-2006

Interpretations of Conflicting Constitutional Sections

3. **Foreign intelligence collection is not assigned to the President or Congress by the Constitution.**

4. **So while “The scope of the President's authority to commit the armed forces to combat is very broad.”**
Memorandum for Honorable Charles W. Colson,
Special Counsel to the President, from William H.
Rehnquist, Assistant Attorney General, Office of Legal
Counsel, *Re: The President and the War Power: South
Vietnam and the Cambodian Sanctuaries* (May 22, 1970)

Most agree it encompass the collection of foreign intelligence in order to carry out military operations.

HOWEVER . . .

Legal Issues 2005-2006

Interpretations of Conflicting Constitutional Sections

United States v. United States District Court for the Eastern District of Michigan et al. (Plamondon et al., Real Parties in Interest), 407 U.S. 297 (June 19, 1972)

Youngstown Sheet and Tube Co. v. Sawyer, 343 U.S. 579 (1952)

1. President acts w/ expressed or implied authorization of Congress.
2. President acts in absence of either Congressional grant or denial of authority.
3. President acts incompatible with expressed or implied will of Congress.

FISA & ECPA

“. . . Except as authorized by statute” 50 U.S.C. § 1809

Legal Issues 2005-2006

Interpretations of Conflicting Constitutional Sections

Authorization for the Use of Military Force, Pub. L. 107-40, 115 Stat. 224 (2001)

Joint resolution authorizing the use of all necessary and appropriate force to engage militarily those responsible for the terrorist attacks of September 11, 2001.

Resolution does not specify what it authorizes as “necessary and appropriate force.”

Legal Issues 2005-2006

Interpretations of Conflicting Constitutional Sections

The Administration's position is that President has Constitutional authority to direct NSA to conduct the activities he described and that this inherent authority is supplemented by the AUMF. Coupled with the Supreme Courts *Hamadi* decision, the President believes he can conduct anywhere in the World, to include within the United States, any activity that can be characterized as a fundamental incident of waging war, to include communication intelligence.

Letter from Assistant Attorney General William E. Moschella to Chairman Roberts and Vice Chairman Rickerfeller of the Senate Select Committee on Intelligence and Chairman Hoekstra and Ranking Minority Member Harman of the House Permanent Select Committee on intelligence (Dec. 22, 2005)

Found at <http://www.freerepublic.com/focus/news/1545787/posts>

Legal Issues 2005-2006

So where are we . . .

Congress- Passed FISA so believe this not exclusively a Presidential Power. Did AUMF authorize conduct? Conflicting along party lines.

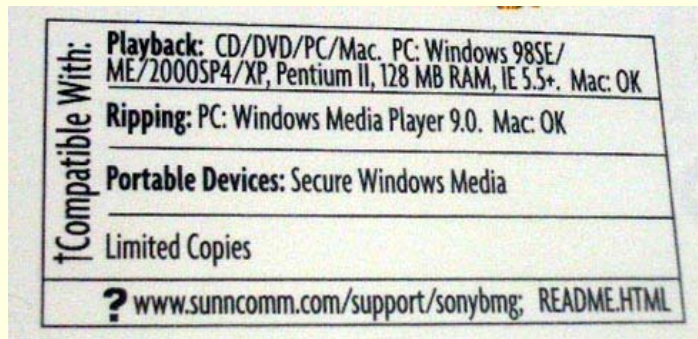
President- Inherent Authority

The Courts (Supremes)- The *Truong* court, as did all the other courts to have decided the issue, held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information. It was incumbent upon the court, therefore, to determine the boundaries of that constitutional authority in the case before it. We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President's constitutional power. The question before us is the reverse, does FISA amplify the President's power by providing a mechanism that at least approaches a classic warrant and which therefore supports the government's contention that FISA searches are constitutionally reasonable.

In re sealed Case, 310 F.3d. 717, 742 (FISA Ct. of Review 2002)

Legal Issues 2005-2006

- Sony BMG



Legal Issues 2005-2006

- **Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004)**
 - District Court Southern District of New York held national security letters are unconstitutional under the First, Fourth, and Fifth Amendments.
 - "John Doe" an internet service provider served with national security letter directing it to turn over information to government relevant to "an authorized investigation to protect against international terrorism." Letter told Doe not to disclose to anyone that a NSL had been issued or records obtained.
 - After consultation with an attorney, Doe withheld the documents requested under the NSL and subsequently brought suit.

Legal Issues 2005-2006

- **Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004)**
 - Doe claimed the broad subpoena power of 2709 violated the First, Fourth, and Fifth Amendments of the Constitution, and that the nondisclosure requirement violated the First Amendment.
 - Court held that, as applied to the ISP, 2709 violates the Fourth Amendment's prohibition on unreasonable search and seizures because 2709 effectively lacks provision for ex post review by a neutral tribunal. In addition, the court noted that the application of 2709 to an ISP may violate that ISP's subscribers' rights to anonymous speech under the First Amendment. Finally, the court concluded that the nondisclosure requirement acts as a prior restraint on speech and a content-based speech restriction in violation of the First Amendment.

Legal Issues 2005-2006

- ***Doe I v. Gonzales*, 2006 U.S. App. LEXIS 12820 (2d Cir. NY. May 23, 2006)**
 - Government seeks review of consolidated cases.
 - John Doe I, SDNY 2709 unconstitutional under the Fourth and First Amendments.
 - John Doe II, United States District Court for the District of Connecticut enjoined enforcement of a gag order on First Amendment grounds

Legal Issues 2005-2006

- ***Doe I v. Gonzales*, 2006 U.S. App. LEXIS 12820 (2d Cir. NY. May 23, 2006)**
 - Section 2709 permitted FBI to issue NSLs to electronic communication service providers, which allowed FBI to gather subscriber information relevant to authorized terrorism investigations.
 - Both John Does received NSLs. After both decisions were rendered, § 2709 was amended by the USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006). Reauthorization Act added provisions that permitted NSL recipients to challenge the issuance of NSLs in court, on appeal, the Fourth Amendment challenges were moot.
 - John Doe I claimed First Amendment issues remained, court remanded this portion of the ruling.
 - John Doe II (gag order preventing disclosure of NSL) on appeal, government rendered this issue moot by asserting that it would not oppose a motion in the district court by the John Doe to modify the non-disclosure requirements so that it could reveal its identity. The court dismissed John Doe II as moot.

Legal Precedents 2005-2006

- ***American Council on Education v. FCC, 2006***
U.S. App. LEXIS 14174 (D.D.C. June 9, 2006)
 - Petitioners sought review of ruling by FCC on the application of the Communications Assistance for Law Enforcement Act, to providers of broadband Internet access and voice over Internet protocol services
 - CALEA, requires "telecommunications carriers" to ensure law enforcement officers could intercept communications carried over their networks and that the FCC could expand the definition of telecommunications carriers to include new technologies that substantially replaced the functions of a local telephone exchange service. FCC found that broadband and VoIP services contained both telecommunications and information components and that CALEA applied to providers of those services to the extent that they qualified **as** telecommunications carriers under the SRP.

Legal Precedents 2005-2006

- **WiFi Crime in Illinois**
- David M. Kauchak, 32, a former Machesney Park resident, is the first person in Winnebago County to be charged with remotely accessing another computer system without the owner's approval. He pleaded guilty Tuesday to the charge and was fined \$250 and sentenced to one year of court supervision.
- "We just want to get the word out that it is a crime. We are prosecuting it, and people need to take precautions," Assistant State's Attorney Tom Wartowski said.

Legal Precedents 2005-2006

- ***Int'l Airports Ctrs., L.L.C. v. Citrin*, 440 F.3d 418 (E.D. Ill. 2005)**
 - Former employer appealed a judgment dismissing its suit brought under the Computer Fraud and Abuse Act against former employee.
 - Employer lent employee a laptop to use for work. Employee decided to quit and go into business for himself, in breach of employment contract. Before returning laptop, employee deleted all the data in it by transmitting a secure-erasure program to the computer, which was designed, by writing over the deleted files, to prevent their recovery. The district court dismissed the employer's suit, but on appeal, the court reversed, finding that whether by Internet download or by disk insertion, a program intended to cause damage was transmitted to the computer electronically. The employee also violated § 1030(a)(5)(A)(ii) because his authorization to access the laptop terminated when he decided to destroy files that incriminated himself and other files that were also the property of his employer in violation of his duty of loyalty.

Legal Precedents 2004-2005

- ***P.C. Yonkers, Inc. v Celebrations the Party & Seasonal Superstore, LLC*, 428 F.3d 504 (3rd Cir. N.J. November 7, 2005)**
 - Employer a franchisees and a management company sued former employees under CFAA and for misappropriation of trade secrets. The district court denied the franchisees' motion for a preliminary injunction. The franchisees appealed.
 - Appellate court agreed with the district court that the employer failed to demonstrate any conduct other than the alleged access; there was no evidence as to what, if any, information was taken. Absent something more than mere access, the employer could not succeed on any of their claims, and injunctive relief was properly denied. The appellate court found, however, that civil relief--including injunctive relief--was available under the CFAA, and it disagreed with the district court to the extent that it opined to the contrary.

Legal Precedents 2004-2005

- ***P.C. Yonkers, Inc. v Celebrations the Party & Seasonal Superstore, LLC*, 428 F.3d 504 (3rd Cir. N.J. November 7, 2005)**
 - The District Court struggled with the meaning of, and relationships among, various provisions of CFAA. The majority of CFAA cases still involve "classic" hacking activities. However, the scope of its reach has been expanded over the last two decades. **"Employers ... are increasingly taking advantage of the CFAA's civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system."** see also *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1124 & n.3 (W.D. Wash. 2000) (explicitly recognizing that Congress' 1994 amendment to the CFAA added a private cause of action under § 1030(g)).

Legal Precedents 2005-2006

- ***Davidoff v. Davidoff*, 2006 N.Y. Misc. LEXIS 1307 (NY Sp Ct May 10, 2006)**
 - Plaintiff commenced action 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.

Legal Precedents 2005-2006

- ***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.

Legal Precedents 2005-2006

- ***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.

Legal Precedents 2005-2006

- ***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]).

Legal Precedents 2005-2006

- ***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.

Legal Precedents 2005-2006

- ***Davidoff v. Davidoff*, 2006 N.Y. Misc. LEXIS 1307 (NY Sp Ct May 10, 2006)**
 - *Citing, Banco Nacional Ultramarino 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.

Legal Precedents 2005-2006

- ***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 and/or plaintiff's Website itself 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 by the defendants. 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.

Legal Precedents 2005-2006

- ***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**

Legal Precedents 2005-2006

- ***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

Legal Precedents 2005-2006

- ***United States v. Garcia*, 2006 U.S. Dist. LEXIS 4642 (W.D. Wisc. February 3, 2006)**
 - **Web Bug/Beacon Debate**
 - **Can Government agencies place (plant) web bugs/beacon into files with the expectation that hackers will download (steal) these files and then reveal their computer's IP Address?**
 - **Search of public space (place)?**
 - **Search of private space (place)?**

Legal Precedents 2005-2006

- ***United States v. Garcia*, 2006 U.S. Dist. LEXIS 4642 (W.D. Wisc. February 3, 2006)**
 - **Before the government may install a locational monitor on the exterior of a person's motor vehicle it must establish *at least* a reasonable suspicion that the car's owner is engaged in criminal activity, and that knowledge of the car's movement in public places will lead to the discovery of evidence relevant to the criminal investigation. As will be come clearer, the reasonable suspicion standard is limited to the installation and monitoring of a transmitter in a public place. Probable cause should be the threshold to allow the government to monitor transmitters inside homes**

Legal Precedents 2005-2006

- ***United States v. Garcia*, 2006 U.S. Dist. LEXIS 4642 (W.D. Wisc. February 3, 2006)**
 - In May 2005, Wisconsin DOJ/DCI agents were investigating Garcia as a suspected methamphetamine cooker in Polk County. Agents knew that Garcia used a silver Ford Tempo. On May 26, 2005, a DCI agent covertly installed a "GPS Memory Tracking Unit" on the exterior of the Tempo (under the rear bumper) while it was parked on a public street. The agent did not obtain a search warrant or a court order before installing the tracking device. By means of satellite trilateration, this device created and stored geographic coordinates commemorating the car's movement

Legal Precedents 2005-2006

- ***United States v. Garcia*, 2006 U.S. Dist. LEXIS 4642 (W.D. Wisc. February 3, 2006)**

- Garcia seeks to suppress all of the evidence against him that was discovered as a result of the agents using a tracking device; this would be everything relevant to the federal indictment. Garcia concedes that he cannot challenge the fact that the agents tracked his car while it was on public streets. *See, e.g., United States v. Knotts*, 460 U.S. 276, 103 S. Ct. 1081, 75 L. Ed. 2d 55 (1983). Garcia limits his challenge to the question left open in *Knotts*: the reasonableness of the warrantless *installation* of a tracking device on his vehicle.

Legal Precedents 2005-2006

- ***United States v. Garcia*, 2006 U.S. Dist. LEXIS 4642 (W.D. Wisc. February 3, 2006)**
 - The government contends that the law is clear (at least in some circuits) that law enforcement agents may install tracking devices on suspects' cars as they see fit, that is with no showing of reasonable suspicion, probable cause, and without a judicial warrant or order.
 - Supreme Court in *United States v. Knotts*, 460 U.S. 276, 103 S. Ct. 1081 (1983), *Fourth Amendment* provides no protection from government using electronic devices surreptitiously to monitor citizen movement in public places.

Legal Precedents 2005-2006

- ***United States v. Garcia*, 2006 U.S. Dist. LEXIS 4642 (W.D. Wisc. February 3, 2006)**
 - Supreme Court fine-tuned *Knotts* in *United States v. Karo*, 468 U.S. 705 (1984), holding that it *did* violate the *Fourth Amendment* for the government to monitor a warrantless tracking device while it was inside a person's private residence.

Legal Precedents 2005-2006

- ***United States v. Garcia*, 2006 U.S. Dist. LEXIS 4642 (W.D. Wisc. February 3, 2006)**
 - Clear from *Karo*, that the government must obtain a court warrant supported by probable cause before *monitoring* a transmitting device that is taken into a private residence. As a practical matter-as noted repeatedly in *dicta* in the cases - it is in the government's best interests always to proceed in this fashion so as not to run the risk that evidence is surrendered because it did not obtain a court order.

Legal Precedents 2005-2006

- ***United States v. Garcia*, 2006 U.S. Dist. LEXIS 4642 (W.D. Wisc. February 3, 2006)**
 - Garcia does have a *Fourth Amendment* right to protect the exterior of his car from government intrusion, but as the courts noted in *Michaels* and *McIver*, the intrusion caused by the application of the device is minimal. The *real* intrusion, which understandably-and justifiably-upset the dissent in *Knotts* is the 24/7 governmental monitoring that follows. However Orwellian and outrageous this may seem, it was settled in favor of the government in *Knotts*.

Legal Precedents 2005-2006

- ***United States v. Garcia*, 2006 U.S. Dist. LEXIS 4642 (W.D. Wisc. February 3, 2006)**
 - *United States v. Jones*, 31 F.3d 1304 (4th Cir. 1994)
 - The Court held it would be a mistake, and a misreading of the Supreme Court's guidance in *Knotts* and *Karo*, to analyze this question solely in terms of Jones' privacy expectation in the interior of his own van. While it agreed that Jones had a reasonable expectation of privacy in the interior of his van, it found no government intrusion there. The beeper was not planted in the van; it was concealed in a mail pouch which belonged to the government and in which Jones had no expectation of privacy whatsoever. The mail pouch with the beeper found its way into Jones' van only because Jones stole the pouch and hid it in the van himself. *Id.* At 1310-11.
- *United States v. Moore*, 562 F.2d 106, 111 (1st Cir 1977), *cert. denied*, 435 U.S. 926 (1978)
 - Fourth Amendment does not prohibit placing of beepers in contraband and stolen goods because possessors of such articles have no legitimate expectation of privacy in substances which they have no right to possess.

Legal Precedents 2005-2006

- ***Island Online, Inc. v. Network Solutions, Inc.*, 119 F. Supp. 2d 289 (E.D. NY 2000)**
 - These addresses, known as “IP addresses,” are similar in function to telephone numbers and are written as a series of no more than 12 digits separated by periods.
- ***United States v. Hambrick*, 2000 U.S. App. LEXIS 18665 (4th Cir. 2000) *cert denied*, 2001 U.S. LEXIS 555 (2001)**
 - What a person knowingly exposes to the public is not a subject of Fourth Amendment protection.

Legal Precedents 2005-2006

- ***In the Matter of Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and a Trap & Trace Device on E-mail Account, 2006 U.S. Dist. LEXIS 4451, (D. D.C. February 2, 2006***
 - Question was did 18 U.S.C.S. §§ 3121-3127 authorized the use of pen register and trap and trace devices on e-mail accounts during criminal investigations. The court held that §§ 3121-3127 authorized use. Court noted the government's application and proposed order afforded sufficient assurances that the contents of the e-mail communications would be protected, the court granted the government's motion and issued its proposed order authorizing the requested pen register and trap and trace devices.

Legal Precedents 2005-2006

■ ***Probation Cases***

■ ***United States v. Lifshitz*, 369 F.3d 173 (2d Cir. NY March 30, 2004)**

■ ***King v. Federal Bureau of Prisons*, 2005 U.S. App. LEXIS 14092 (7th Cir. Ill. July 13, 2005)**

■ ***United States v. Balon*, 384 F.3d 38; (2d Cir. NY September 20, 2004)**

■ ***United States v. Yuknavich*, 419 F.3d 1302 (11th Cir. N.D. Ga. August 11, 2005)**

■ ***United States v. Parson* (W.D. Wash. January 28, 2005)**

■ ***Real World Friends***

Arrests, Indictments & Prosecutions 2005-2006

- **Kenneth Kwak, Department of Education Office of Inspector General, Computer Security Specialist**
- **Scott Levine, Controlling Owner Snipermail, Inc. (aka Dr. Evil)**
- **You Li, Chinese National, Undergrad U of Utah (aka this is not Ferris Bueller)**
- **Jeanson James Ancheta, Botmaster underground, (aka Do a B O T lose a B M W)**
- **Carlos Enrique Perez-Melara (aka Loverspy)**

Contact Information

- Major Robert Clark
- 703-706-2247
- rclark@1stiocmd.army.mil