

**Legal Aspects of
Computer Network Defense-
A Government Prospective
&
A Year In Review
Precedents in Computer and Internet
Security Law
2004-2005**

**Black Hat Briefings
USA 2005
July 27, 2005
Major R.W. Clark
U.S. Army, JAGC**

Agenda

- **History**
- **Computer Network Defense**
- **Computer Crime Prosecutions, Arrests & Indictments July 2004 to June 2005**
- **Computer & Internet Legal Precedents July 2004 to June 2005**
- **Issues in Computer & Internet Security**

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.*

Disclaimer

aka What's Not Here

- **Super Secret Government Things**
- **Double Secret Probation Things**
- **Confessions That We Really Were the Ones That Crashed Your System**
- **Confessions on Area 51 or Aliens**
 - **Although Great Computer Technology!!**

What is Here

- **Understanding of Government Computer Network Defense**
- **Understanding of Recent Precedents**
- **Understanding of some legal theories that pertain to areas of computer and Internet security**

Final Disclaimer aka I'm Not Your Lawyer

- **Legal Argument Which authorizes Use of Beacons/Honeypots/Active Response**
- **Legal Advice Deals With Risk Management**

History

Courts Discover “computer”

- 1900 – 1910 11
- 1910 – 1920 7
- 1920 – 1930 3
- 1930 – 1940 10
- 1940 – 1950 13
- 1950 – 1960 24
- 1960 – 1970 411
- 1970 – 1980 4,268
- 1980 – 1990 15,513
- 1990 – 2000 36,122
- 2000 – May 1, 2005 30,216

History

Computers Recognized by the Courts

- ***Comptograph Co. v. Universal Accountant Mach. Co.***, 142 F. 539 (N.D. Ill. January 19, 1906)
- ***In re Spitzglass***, 96 F. 2d 1002 (C.C.P.A. June 6, 1938)
- ***Sperry Rand Corp. v. Bell Tel. Labs.***, 171 F. Supp. 343 (S.D.N.Y. March 19, 1959)
- ***Sperry Rand Corp. v. Bell Tel. Labs.***, 208 F. Supp. 598 (S.D.N.Y. September 6, 1962) *appeal dismissed*, 317 F. 2d 491, 493 (2d Cir. NY 1963)
- ***Eckert v. Commissioner***, 19 T.C.M. (CCH) 1465 (November 30, 1960)

History

Hacking Invented

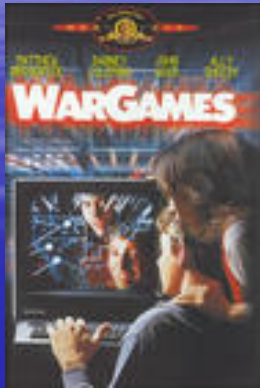
- **1960s The Dawn of Hacking**
 - MIT & “Hack”
- **1970s**
 - Phone Phreaks and Cap'n Crunch
- **1980s**
 - Hacker Message Boards and Groups
 - The 414 gang - six teenagers
 - CFAA & Morris
- **1990s**
 - Poulsen, Def Con, Minnick oh my!
- **2000s**
 - Like you don't remember!

History

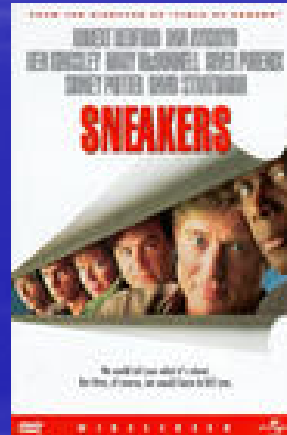
2001: A Space Odyssey 1968



Wargames 1983



Sneakers 1992



The Net 1995



Hackers
1995

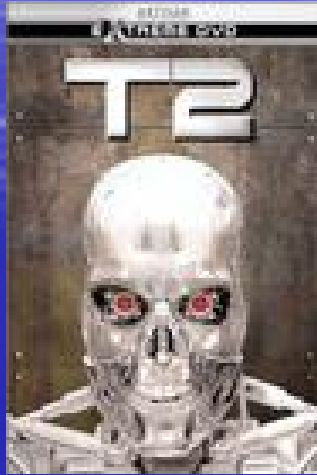


History

The Terminator 1984



Terminator 2: Judgment Day 1991



Terminator 3: Rise of the Machines 2003



In the future, Skynet, a computer system fights a losing war against the humans who built it and who it nearly exterminated. Just before being destroyed, Skynet sends a Terminator back in time to kill Sarah, the mother to be of John Connor, the Leader of the human resistance. The terminator can pass for human, is nearly indestructible, and has only one mission, killing Sarah Connor. One soldier is sent back to protect her from the killing machine. He must find Sarah before the Terminator can carry out it's mission

<http://www.imdb.com/>

Authority for Computer Network Defense

- **Common Law Principle**
- **Property is “the free use, enjoyment, and disposal of all his acquisitions, without any control or diminution, save only by the laws of the land.”**
 - George J. Siedel, *Real Estate Law* 21 (1979), *citing*, W. Blackstone, *Commentaries* 138
- **Property in its nature is an unrestricted and exclusive right. Hence it comprises in itself the right to dispose of the substance of the thing in every legal way, to possess it, to use it, and to exclude every other person from interfering with it.**
 - Mackeldey, *Roman Law* § 265 (1883).

Authority for Computer Network Defense

- Right to exclude people from one's personal property is not unlimited.
- 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)

Authority for Computer Network Defense

- A typical defense of-property statute provides that “one is justified in using reasonable force to protect his property from trespass or theft, when he reasonably believes that his property is in immediate danger of such an unlawful interference that the use of such force is necessary to avoid the danger.”
 - Susan Michelle Gerling, *Louisiana's New "Kill the Carjacker" Statute: Self-Defense or Instant Injustice?*, 55 Wash. U. J. Urb. & Contemp. L. 109,120 (1999), *citing*, Wayne R. LaFave & Austin W. Scott, Jr., *Criminal Law* 5.9 at 667 (2d Ed. 1986).

Authority for Computer Network Defense

- Common Law Doctrine-Trespass to Chattel
- *Intel v. Hamidi*, 71 P.3d 296 (Cal. Sp. Ct. June 30, 2003)
- *Pearl Investments v. Standard I/O, Inc.*, 257 F. Supp. 2d 326 (D. Me. April 2, 2003)
- *Ticketmaster Corp., v. Tickets.Com, Inc.*, 2003 U.S. Dist. LEXIS 6483 C.D. Cal. March 6, 2003)
- *Tyco International v. John Doe*, 2003 U.S. Dist. LEXIS 25136 (S.D. N.Y. August 29, 2003)

Authority for Computer Network Defense

- (U) Executive Order 13231, Critical Infrastructure Protection in the Information Age, October 18, 2001
- **Defense Information Assurance Program, 10 U.S.C. § 2224 (West 2005)**
- (U) DODD O-8500.1, Information Assurance (IA), October 24, 2002
- (FOUO) DODD O-8530.1, Computer Network Defense (CND), January 8, 2001
- (FOUO) DODD O-8530.2, Support to Computer Network Defense, March 9, 2001

Authority for Computer Network Defense

- (U) CJCSI 6510.01D, Information Assurance (IA) and Computer Network Defense (CND), June 15, 2004
- (U) CJCSM 6510.01, Defense in Depth: Information Assurance (IA) and Computer Network Defense (CND), March 25, 2003
- (U) AR 25-2, Information Assurance, November 14, 2003
- (U) Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a) (West 2005)
- **Electronic Communication and Privacy Act, 18 U.S.C. § 2510 et seq., (West 2005)**
- **Pen Registers and Trap Devices, 18 U.S.C. § 3121 et seq., (West 2005)**

Department of Defense

Computer Network Defense

- **United States Strategic Command will:**
 - Direct DOD-wide CND operations to defend DOD computer networks.
 - Develop coordinated defensive response actions necessary for a synchronized defense of DOD computer networks in response to unauthorized activity.
 - (U) CJCSI 6510.01D, Information Assurance (IA) and Computer Network Defense (CND), 15 June 2004, Enclosure C, paragraph 3, Commander US Strategic Command Responsibilities

Department of Defense

Computer Network Defense

- Actions taken to **protect, monitor, analyze, detect, and respond** to unauthorized activity **within** DoD information systems and computer networks
- **Monitoring, analysis, detection** activities, including trend and pattern analysis, are **performed by multiple disciplines** within the Department of Defense, e.g., network operations, CND Services, intelligence, counterintelligence and law enforcement.
 - CJCSI 6510.01D

Department of Defense

Computer Network Defense

- **Multiple disciplines** use their **inherent capabilities** and accomplish specific CND actions within their larger functional areas to defend DOD computer networks... CND requires **close coordination** between Network operations (CERTs/NOSCs), intelligence, communications, counterintelligence and law enforcement to successfully defend DOD computer networks.
 - CJCSI 6510.01D

Department of Defense

Computer Network Defense

**Event Will Determine DOD Response
and Legal Authority**

- **Multiple disciplines**
 - **Network Ops-
CERTs/NOSCs**
 - **Intelligence**
 - **Counterintelligence**
 - **Law enforcement**
 - **Commander-in-
Chief**

Army CERT Computer Network Defense

- (1) ensure proper performance under **service provider exception** in the normal course of employment to keep the service operational/ protect the rights or property.
- (2) authorized to use **CIO/G-6-approved** automated monitoring **tools** . . . SA/NA does not have unlimited authority in the use of these monitoring tools. . . . tools are used only for their intended purpose.
- (3) discover possible **criminal offense**, immediately **report to LEA**
- (4) Only LE/CI personnel are authorized to intercept the content of an individual's communication, after obtaining appropriate legal authority
 - AR 25-2, paragraph 4-5t

Army CERT Computer Network Defense

- 18 U.S.C. § 2511(2)(a)(i)
 - “may intercept or disclose communications on its own machines “in the **normal course** of employment while engaged in any activity which is a **necessary** incident to . . . the **protection of the rights or property** of the provider of that service.”

Private Organization Computer Network Defense

- 18 U.S.C. § 2511(2)(a)(i)
 - “may intercept or disclose communications on its own machines “in the **normal course** of employment while engaged in any activity which is a **necessary** incident to . . . the **protection of the rights or property** of the provider of that service.”

Computer Network Defense

- **The Service Provider Exception is a limited exception. Not a criminal investigator's privilege.**

18 U.S.C. § 2511(2)(a)(i)

Computer Network Defense

- Broad exception, however, Provider must conduct reasonable, tailored monitoring to protect itself from harm.
- **Doesn't allow unlimited monitoring**
 - Need “substantial nexus” b/w threat and property
 - *U.S. v McLaren*, 957 F. Supp 215, 219 (M.D. Fla. 1997)
- System administrators **can track hackers** within their networks in order to prevent further damage.
 - *U.S. v Mullins*, 992 F.2d 1472, 1478 (9th Cir. 1993)

Computer Network Defense

- **Notification of Monitoring**
- **Banners**
- **Computer Use Policies**

Legal Precedents 2004- 2005

- *In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 2005 Bankr. LEXIS 415 (Bankr. S.D.N.Y. March 21, 2005)(As Amended, March 23, 2005)

Legal Precedents 2004- 2005

- *Borninski v. Williamson*, 2005 U.S. Dist. LEXIS 9401 (N.D. Tex. May 17, 2005)

Legal Precedents 2004-2005

- *In the Matter of the Application of the United States for a Nunc Pro Tunc Order for Disclosure of Telecommunications Records*, 352 F. Supp. 2d 45 (D. Mass. January 3, 2005)

Legal Precedents 2004-2005

- *Freedman v. Am. Online, Inc*, 329 F. Supp. 2d 745 (E.D. Va. August 11, 2004)
- *Freedman v. Am. Online, Inc.*, 303 F. Supp. 2d 121 (D. Conn. February 4, 2004)
- *Fitch v. Doe*, 869 A.2d 722, (Me. Sp. Ct. January 11, 2005)

Legal Precedents 2004-2005

- *United States v. Long*, 2005 CCA LEXIS 155, (U.S.N.M.C.C.C.A. May 11, 2005)
- *United States v. Maxwell*, 45 M.J. 406, (C.A.A.F. 1996)
- *United States v. Hambrick*, 55 F. Supp. 2d 504 (W.D. Va. July 7, 1999)
 - The defendant cites *United States v. Maxwell*, 45 M.J. 406 (C.A.A.F. 1996) as the only published federal decision that deals with the question of the expectation of privacy in information obtained from an ISP. Although some of the facts of *Maxwell* appear to be similar to the facts in the present case, ***Maxwell* has little or no precedential value because the United States Court of Appeals for the Armed Forces decided the case.** That court reviews the convictions of a court-martial and is entirely separate from the United States Courts of Appeals.

Legal Precedents 2004- 2005

- ***United States v. Plush*, 2004 CCA LEXIS 230 (U.S.A.F.C.C.A. September 21, 2004)**
- ***State v. Lasaga*, 269 Conn. 454; 848 A.2d 1149 (Jun. 1, 2004)**

DoD's Active Response

Law Enforcement

- **Investigation of a crime**
 - **Constitution, 4th Amendment**
 - **Domestic Statutes**

Intelligence Community

- **Intelligence Organizations**
- **E.O. 12333**
- **DoDD 5240.1, DoDD 5240.1-R**
- **Foreign Intelligence Surveillance Act**

Commander-in-Chief Authority

- **Constitution**
- **Standing Rules of Engagement**
 - CJCSI 3121.01A, Enclosure F, 15 JAN 2000
- **Hostile act/intent**
- **Use of Force**
- **Article 2(4) refrain from threat or use of force**
- **Article 39 Security Council Determination**
- **Article 51 Self Defense in response to “armed attack”**
 - **Necessity & proportionality**

Arrests, Indictments & Prosecutions 2004-2005

- *United States v. Sabathia* (E.D. Cal. July 28, 2004)
- Charges- charged with ten counts of fraudulently using her computer to embezzle more than \$875,035 from North Bay Health Care Group
- Why- She pled guilty during this conference last year
- Sentence- Potential 5 years; fine \$250,000

Arrests, Indictments & Prosecutions 2004-2005

- *United States v. Salcedo* (W.D. N. Car. December 15, 2004)
- Charges- Pled to 4 Counts of 14 Count Indictment- Unlawful Access to Lowe's Nationwide Computer System
- Sentenced to 108 months imprisonment longest since Kevin Mitnick's 68-months
- *United States v. Botbyl* (W.D. N.Car. December 15, 2004)
- Charges- Pled to Count One, Conspiracy
- Sentenced to 26 months imprisonment
- *United States v. Timmins* (W.D. N. Car. April 2005)

Arrests, Indictments & Prosecutions 2004-2005

- *United States v. Jiang* (S.D.N.Y. February 28, 2005)
- Charges- Pled to 5 Counts relating to computer fraud and software piracy involving Kinko's Inc.
- Sentenced to 27 months imprisonment followed by 3 years supervised release.

Arrests, Indictments & Prosecutions 2004-2005

- *United States v. Trowbridge* (Wash. D.C. January 18, 2005) & *United States v. Chicoine* (Wash. D.C. January 18, 2005)
- Charges- Pled to 1 Count of conspiracy to commit felony criminal copyright infringement (P2P)
- Sentence- Potential- 5 years; fine \$250,000

Arrests, Indictments & Prosecutions 2004-2005

- *United States v. Tanner* (Wash. D.C. January 18, 2005)
- Charges- Pled to 1 Count of conspiracy to commit felony criminal copyright infringement (P2P)
- Sentence- Potential- 5 years; fine \$250,000

Arrests, Indictments & Prosecutions 2004-2005

- *United States v. Greco* (C.D. Cal. March 22, 2005)
- Charges- Pled to 1 Count of threatening to damage the computer system of Myspace.com (CAN-SPAM)
- SPIM
- Sentence- Potential- 5 years

Arrests, Indictments & Prosecutions 2004-2005

- *United States v. Lytle* (N.D. Cal. March 11, 2005)
- Charges- Pled to 5 Counts of computer crimes in violation of 18 U.S.C. § 1030.
- Sentence- Potential- 10 years; fine \$250,000; 5 years; fine \$250,000; 1 year; fine \$100,000

Arrests, Indictments & Prosecutions 2004-2005

- *United States v. Mantovani* (N.J. October 28, 2004)
- Charges- 19 Individuals; 62 Count Indictment; computer hacking; dissemination of stolen credit card, debit card and bank account numbers and counterfeit identification documents, such as drivers' licenses, passports and Social Security cards; conspiracy to commit "carding" the use of account numbers and counterfeit identity documents to complete identity theft and defraud banks and retailers; 61 counts unlawful trafficking in stolen credit card numbers and other access devices, unlawful transfer of identification documents to facilitate unlawful conduct, transferring false identification documents and unauthorized solicitation to offer access devices
- Sentence- Potential- ranging from three to 15 years in prison

Arrests, Indictments & Prosecutions 2004-2005

- *United States v. Parson* (W.D. Wash. January 28, 2005)
- Charges- Pled to intentionally causing and attempting to cause damage to a protected computer (Variant of MSBlaster Worm)
- Sentence- 18 months; 3 years supervised release; no video games, no chat rooms; no anonymous friends; real world friends

Arrests, Indictments & Prosecutions 2004-2005



Alex Rodriguez, #13-3B



- *United States v. Rodriguez*, (S.D.N.Y. August 17, 2004)
- Okay not the MLB player, but...

Arrests, Indictments & Prosecutions 2004-2005

- *United States v. Rodriguez*, (S.D.N.Y. August 17, 2004)
- Alex Rodriguez arrested alleged sale and supplying others with pirated computer software in Manhattan.
- Operates a stand on East 14th Street
- Twice sold pirated software to undercover FBI agent
- Supplied illegal computer software to another individual who operated a stand on East 23rd Street
- Faces a maximum sentence of 10 years in prison and a fine of \$250,000 or twice the gross gain or gross loss from the offense.

Legal Precedents 2004- 2005

- METRO-GOLDWYN-MAYER STUDIOS, INC.; COLUMBIA PICTURES INDUSTRIES, INC.; DISNEY ENTERPRISES, INC.; PARAMOUNT PICTURES CORPORATION; TWENTIETH CENTURY FOX FILM CORPORATION; UNIVERSAL CITY STUDIOS LLP, f/k/a Universal City Studios, Inc.; NEW LINE CINEMA CORPORATION; TIME WARNER ENTERTAINMENT COMPANY, LP; ATLANTIC RECORDING CORPORATION; ATLANTIC RHINO VENTURES, INC., d/b/a Rhino Entertainment, Inc.; ELEKTRA ENTERTAINMENT GROUP, INC.; LONDON-SIRE RECORDS, INC., LP; WARNER BROTHERS RECORDS, INC.; WEA INTERNATIONAL INC.; WARNER MUSIC LATINA, INC., f/k/a WEA Latina, Inc.; ARISTA RECORDS, INC.; BAD BOY RECORDS; CAPITOL RECORDS, INC.; HOLLYWOOD RECORDS, INC.; INTERSCOPE RECORDS; LAFACE RECORDS; MOTOWN RECORD COMPANY; RCA RECORDS LABEL, a unit of BMG Music d/b/a BMG Entertainment; SONY MUSIC ENTERTAINMENT, INC.; UMG RECORDINGS, INC.; VIRGIN RECORDS AMERICA, INC.; WALT DISNEY RECORDS, a division of ABC, Inc.; ZOMBA RECORDING CORP., Plaintiffs-Appellants, v. GROKSTER LTD.; STREAMCAST NETWORKS, INC., f/k/a Musiccity.Com, Inc., Appellees, and SHARMAN NETWORKS LIMITED; LEF INTERACTIVE PTY LTD., Defendants. JERRY LEIBER, individually d/b/a Jerry Leiber Music; MIKE STOLLER, individually and d/b/a Mike Stoller Music; PEER INTERNATIONAL CORPORATION, PEER MUSIC LTD., SONGS OF PEER LTD.; CRITERION MUSIC CORPORATION; FAMOUS MUSIC CORPORATION, BRUIN MUSIC COMPANY; ENSIGN MUSIC CORPORATION; AND LET'S TALK SHOP, INC., d/b/a Beau-DI-O-DO Music, on behalf of themselves and all other similarly situated, Plaintiffs-Appellants, v. CONSUMER EMPOWERMENT BV, aka Fasttrack; SHARMAN NETWORKS LIMITED; LEF INTERACTIVE PTY LTD., Defendants, and GROKSTER LTD.; STREAMCAST NETWORKS, INC., f/k/a Musiccity.Com, Inc., Defendants-Appellees. METRO-GOLDWYN-MAYER STUDIOS, INC.; COLUMBIA PICTURES INDUSTRIES, INC.; DISNEY ENTERPRISES, INC.; PARAMOUNT PICTURES CORPORATION; TWENTIETH CENTURY FOX FILM CORPORATION; UNIVERSAL CITY STUDIOS LLP, f/k/a Universal City Studios, Inc.; NEW LINE CINEMA CORPORATION; TIME WARNER ENTERTAINMENT COMPANY, LP; ATLANTIC RECORDING CORPORATION; ATLANTIC RHINO VENTURES, INC., d/b/a Rhino Entertainment, Inc.; ELEKTRA ENTERTAINMENT GROUP, INC.; LONDON-SIRE RECORDS, INC., LP; WARNER BROTHERS RECORDS, INC.; WEA INTERNATIONAL INC.; WARNER MUSIC LATINA, INC., f/k/a WEA Latina, Inc.; ARISTA RECORDS, INC.; BAD BOY RECORDS; CAPITOL RECORDS, INC.; HOLLYWOOD RECORDS, INC.; INTERSCOPE RECORDS; LAFACE RECORDS; MOTOWN RECORD COMPANY; RCA RECORDS LABEL, a unit of BMG Music d/b/a BMG Entertainment; SONY MUSIC ENTERTAINMENT, INC.; UMG RECORDINGS, INC.; VIRGIN RECORDS AMERICA, INC.; WALT DISNEY RECORDS, a division of ABC, Inc.; ZOMBA RECORDING CORP., Plaintiffs-Appellants, v. GROKSTER LTD.; STREAMCAST NETWORKS, INC., f/k/a Musiccity.Com, Inc., Defendants-Appellees.

Legal Precedents 2004-2005

- ***MGM Studios, Inc v Grokster Ltd.***, 380 F.3d 1154 (9th Cir. Cal. August 19, 2004)(*cert. granted by MGM Studios v. Grokster, Ltd.*, 160 L. Ed. 2d 518, 125 S. Ct. 686, (Dec. 10, 2004))

Legal Precedents 2004-2005

- *United States v. Councilman*, 245 F. Supp. 2d 319 (D. Mass. February 12, 2003) affirmed in *United States v. Councilman* 373 F.3d 197 (1st Cir. Mass. 2004) Opinion vacated and withdrawn in *United States v. Councilman* 385 F.3d 793, 2004 U.S. App. LEXIS 20756 (1st Cir. 2004).
- *Hall v. Earthlink Networks, Inc.*, 396 F. 3d 500 (2d Cir. N.Y. January 25, 2005)

Legal Precedents 2004- 2005

- ***United States v. Mitra*, 2005 U.S. App. LEXIS 6717 (7th Cir. Wisc. April 18, 2005)**

Legal Precedents 2004-2005

- *Charter Communs., Inc., Subpoena Enforcement Matter v. Charter Communs., Inc*, 393 F.3d 771 (8th Cir. Missouri January 4, 2005) *Rehearing denied by, Rehearing, en banc, denied by Recording Indus. Ass'n of Am. v. Charter Communs., Inc.*, 2005 U.S. App. LEXIS 5599 (8th Cir., Apr. 6, 2005).

Legal Precedents 2004-2005

- *Recording Industry Association of America v. Verizon Internet Services, Inc.*, 359 U.S. App. D.C. 85 (D.C. Cir. December 19, 2003)(As **Amended January 16, 2004**. Rehearing, en banc, denied by *Recording Industry Association of America v. Verizon Internet Services, Inc.*, 2004 U.S. App. LEXIS 3564 (D.C. Cir. February 24, 2004) Rehearing denied by *Recording Industry Association of America v. Verizon Internet Services, Inc.*, 2004 U.S. App. LEXIS 3563 (D.C. Cir. **February 24, 2004**)(Costs and fees proceeding at, Request granted *Recording Industry Association of America v. Verizon Internet Services, Inc.*, 2004 U.S. App. LEXIS 4952 (D.C. Cir. **March 15, 2004**)(Certiorari denied by *Recording Industry Association of America v. Verizon Internet Services, Inc.*, 2004 U.S. LEXIS 6700 (U.S., **Oct. 12, 2004**))(Certiorari denied by *Recording Industry Association of America v. Verizon Internet Services, Inc.*, 2004 U.S. LEXIS 6701 (U.S., **Oct. 12, 2004**)
Prior History- Appeals from the United States District Court for the District of Columbia. *Recording Industry Association of America v. Verizon Internet Services, Inc.*, 2003 U.S. App. LEXIS 11250 (D.C. Cir. June 4, 2003)

Legal Issues

Web Bugs/Beacons

- 18 U.S.C. § 3121
- 18 U.S.C.S. § 3121(b)
 - 1 ISP
 - 2 ISP
 - 3 Consent
- *Smith v. Maryland*, 442 U.S. 735, 743-744 (1979)
- *Island Online, Inc., v. Network Solutions, Inc.*, 119 F. Supp. 2d 289 (E.D.N.Y. November 6, 2000)
- *United States v. Hambrick*, 2000 U.S. App. LEXIS 18665 (4th Cir. Va. August 3, 2000)

Legal Issues

Web Bugs/Beacons

- *In Re Toys R Us Inc., Privacy Litigation*, 2001 U.S. Dist. LEXIS 16947 (N.D. Cal. 2001)
- *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 501-02 (S.D.N.Y. March 29, 2001)
- *In re Pharmatrak, Inc. Privacy Litigation*, 292 F. Supp. 2d 263 (D. Mass. November 6, 2003)
- *In re Pharmatrak, Inc. Privacy Litigation*, 329 F.3d 9 (1st Cir. Mass. May 9 2003)
- *United States v. Jones*, 31 F.3d 1304 (4th Cir. 1994)
- *United States v. Petersen*, 98 F.3d 502 (9th Cir. Cal. October 22, 1996)

Legal Issues

Active Response



Legal Issues

Active Response

- *Katko v Briney*, 183 N.W. 2d 657 (1971)
- 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

Legal Issues

Active Response

- *Gross v. Taylor*, 1997 U.S. Dist LEXIS 11657 (E.D. Pa. August 5, 1997)(mere possession of interception equipment fails to show that defendant actually received or intercepted plaintiff's communication)
- Targeting
- *Island Online, Inc., v. Network Solutions, Inc.*, 119 F. Supp. 2d 289 (E.D.N.Y. November 6, 2000)
- *United States v. Petersen*, 98 F. 3d 502 (9th Cir. Cal. October 22, 1996)

Legal Issues

Active Response

- **Law of Necessity**
 - Target
 - Proportionality
 - Necessity

Year in review 2004-2005

House Proposed Legislation

- **HR 29 SPYACT**
- **HR 285 Dept of Homeland Security Cybersecurity Enhancement Act of 2005**
- **HR 744 Internet Spyware (I-SPY) Prevention Act of 2005**
- **HR 1069 Notification of risk to personal data act**
- **HR 1099 Anti-phishing Act of 2005**
- **H. R. 1189, Personal Pictures Protection Act of 2005, 2005 H.R. 1189; 109 H.R. 1189**
- **HR 1263 Consumer Privacy Protection Act of 2005**
- **HR 1558 Computer-Assisted Remote Hunting Act**

Year in review 2004-2005

Senate Proposed Legislation

- **S 115 (Jan 24, 2005) Notification of Risk to Personal Data Act**
- **S 116 Privacy Act of 2005**
- **S 318 Computer Trespass Clarification Act of 2005**
- **S 472 Anti-phishing Act of 2005**
- **S 687 Software Principles Yielding Better Levels of Consumer Knowledge Act or SPY BLOCK Act**
- **S 737 Security and Freedom Enhancement Act of 2005 or SAFE Act**
- **S 751 Apr 14, 2005 Notification of Risk to Personal Data Act Same as S 115**
- **S 768 Comprehensive Identity Theft Prevention Act**
- **S 849 Internet Tax Nondiscrimination Act,**

Year in review 2004-2005

Statutory Law Update

- National Security Information
- 18 U.S.C. § 1030 (a) (1) **access/exceed authorization; obtain information; injury of the United States/advantage foreign nation, and communicates, delivers, transmits, or cause same or attempt same; or willfully retains**
 - 18 U.S.C. § 1030(c)(1)(A) Punishment
 - **1st Offense Fine and/or 10 years**
 - **2nd Offense Fine and/or 20 years**

Year in review 2004-2005

Statutory Law Update

- 18 U.S.C. § 1030 (a)(2) **accesses/exceeds** to obtains:
 - (A) **information** in **financial institution**/card issuer;
 - (B) information of the **United States**; or
 - (C) information from **protected computer**
- 18 U.S.C. § 1030(c)(2)(A) Punishment
 - **1st Offense Fine and/or 1 years**
 - **2nd Offense Fine and/or 10 years**
 - 18 U.S.C. § 1030(c)(2)(B) if
 - (i) done for commercial advantage or financial gain;
 - (ii) done in furtherance of criminal or tortious act; or
 - (iii) value of the information obtained exceeds \$ 5,000
 - **1st Offense Fine and/or 5 Years**
 - **2nd Offense Fine and/or 10 Years**

Year in review 2004-2005

Statutory Law Update

- **Trespass of Government Systems**
- **18 U.S.C. § 1030 (a)(3) access nonpublic computer of United States or computer exclusively for the use of the Government of the United States**
- **18 U.S.C. § 1030(c)(2)(A) Punishment**
 - **1st Offense Fine and/or 1 years**
 - **2nd Offense Fine and/or 10 years**

Year in review 2004-2005

Statutory Law Update

- Fraud
- 18 U.S.C. § 1030 (a)(4) exceeds/accesses a protected computer to further an intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$ 5,000 in any 1-year period
- 18 U.S.C. § 1030(c)(3)(A) Punishment
 - **1st Offense Fine and/or 5 years**
 - **2nd Offense Fine and/or 10 years**

Year in review 2004-2005

- Intrusion **Statutory Law Update**
- 18 U.S.C. § 1030 (a)(5) (A) (i) causes the transmission of a program, information, code, or command, result of such conduct, intentionally causes damage to a protected computer
 - 18 U.S.C. § 1030(c)(4)(A) Punishment
 - **1st Offense Fine and/or 10 years**
 - 18 U.S.C. § 1030(c)(5)(A) Punishment
 - **If causes serious bodily injury Fine and/or 20 years**
 - 18 U.S.C. § 1030(c)(5)(B) Punishment
 - **If causes death Fine and/or any terms of years or life**

Year in review 2004-2005

Statutory Law Update

- Intrusion
- 18 U.S.C. § 1030 (a)(5)(A)(ii) accesses a protected computer and as a result of such conduct, **recklessly causes damage**
- 18 U.S.C. § 1030(c)(4)(B) Punishment
 - **1st Offense Fine and/or 5 years**
- 18 U.S.C. § 1030(c)(4)(C) Punishment
 - **2nd Offense Fine and/or 20 years**

Year in review 2004-2005

Statutory Law Update

- Intrusion
- 18 U.S.C. § 1030 (a)(5)(A)(iii) accesses a protected computer and as a result of such conduct, **causes damage**
- 18 U.S.C. § 1030(c)(2)(A) Punishment
 - **1st Offense Fine and/or 1 years**
- 18 U.S.C. § 1030(c)(3)(B) Punishment
 - **2nd Offense Fine and/or 10 years**

Year in review 2004-2005

Statutory Law Update

- 18 U.S.C. § 1030 (a)(5)(A)(ii) and (iii) required recklessly cause damage or causes damage is:
- 18 U.S.C. § 1030(a)(5)(B):by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused
 - (i) loss to 1 or more persons during 1-year period aggregating at least \$ **5,000** in value;
 - (ii) **modification**/impairment of **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 computer used in justice, defense, security

Year in review 2004-2005

Statutory Law Update

- Password Trafficking
- 18 U.S.C. § 1030 (a)(6) traffics in any password or similar information through which a computer may be accessed without authorization
- 18 U.S.C. § 1030(c)(2)(A) Punishment
 - **1st Offense Fine and/or 1 years**
- 18 U.S.C. § 1030(c)(3)(B) Punishment
 - **2nd Offense Fine and/or 10 years**

Year in review 2004-2005

Statutory Law Update

- Extortion
- 18 U.S.C. § 1030 (a)(7) intent to extort from any person any money or other thing of value, transmits any communication containing any threat to cause damage to a protected computer
- 18 U.S.C. § 1030(c)(3)(A) Punishment
 - **1st Offense Fine and/or 5 years**
- 18 U.S.C. § 1030(c)(3)(B) Punishment
 - **2nd Offense Fine and/or 10 years**

Year in review 2004-2005

Statutory Law Update

- **Attempts**
- **18 U.S.C. § 1030 (b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.**

Final Thoughts Regarding Active Response

- **Katko v Briney, 183 N.W. 2d 657
(1971)**
 - **EDWARD BRINEY and BERTHA L.
BRINEY**

Contact Information

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