A Year In Review:

Precedents in Computer and Internet Security Law 2008-2009

DEFCON 17
July 31, 2009
R.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.**

Fortunately US Sentencing Commission will not recognizes your special skills

- **Feds won't deem proxies 'sophisticated'**
- **US government has dropped --for now--a plan to classify the use of "proxy“ servers as evidence of sophistication in committing a crime.**
- **US Sentencing Commission was considering a change to federal sentencing guidelines that would have increased sentences by about 25 percent for people convicted of crimes in which proxies are used to hide the perpetrators' tracks.**
- **Digital-rights advocates complained language too broad**
- **Commission struck the controversial language from the amendments**
- **Justice Department supported the proposed amendment as a way to hand down stiffer sentences for people who set up elaborate proxy networks--sometimes in multiple countries --to commit crimes and hide their identities.**
- **Digital-rights advocates said the amendment would have sent a chilling message about using a common technology that is often encouraged as a safer way of using the Internet.**

Agenda

- Encrypted Hard Drive
- Scope of Consent & Investigation
- Untimely Search after Seizure
- Consent/Destruction of Evidence/Revoke consent to search computer
- Border Search of PC Away from Border
- FTC and Cyberspy Software
- Installing viruses and key stroke logger
- Responsible Disclosure
- Cyberwarfare and Definitions
- What Makes a Hacker – 2 operating systems
- Spoliation of evidence can equal losing case
- Anonymity
- Swinging scale of CFAA
- Possession of malware/Reverse engineering

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

Army CERT

Navy CIO

US-CERT

In re: Grand Jury Subpoena to Sebastien Boucher, 2009 U.S. Dist. LEXIS 13006 (DC Ver. Feb. 19, 2009)

- **Gov't appeal US Magistrate Judge's Opinion and Order granting Defendant's motion to quash grand jury subpoena that it violates his Fifth Amendment right.**
- **Gov't doesn't want password for encrypted HD wants only to have defendant provide an unencrypted version of the HD to grand jury.**
- **Court –Boucher must provide an unencrypted version of HD to grand jury.**
- **Acts of producing incriminating 2 situations – 1 existence and location unknown to Gov't; 2 production implicitly authenticates.**
- **Gov't knows incriminating files on encrypted drive Z: and will not use this as "authentication" will link files to Defendant in other way**

United States v. Richardson, 2008 U.S. Dist LEXIS 88242 (W.D. Penn. Oct 31, 2008)
United States v. Parson, 2009 U.S. Dist. LEXIS 15125 (W.D. Penn. Feb. 25, 2009)

- **ICE Agents**
- **Investigating Child Porn**
- **Knock and Talk**
- **Victim of identity theft**
- **Can we search your computer for evidence of identity theft**
- **Scope of consent**

United States v. Mitchell, 2009 U.S. App. LEXIS 8258 (11th Cir. Ga. Apr. 22, 2009)

- **ICE Knock & Talk - Child porn investigation**
- **Defendant admits computer contains child porn but does not give consent to search**
- **ICE agents open up computer and seize HD.**
- **Sits unsearched for 3 weeks until lead agent applied for and gets warrant to search it**
- **Agent out of office for 2 weeks on training, not in hurry**
- **Conviction vacated, evidence suppressed, initial seizure justified, delay in obtaining search authorization not within a reasonable period of time**

United States v. Knighton, Sr., 2009 U.S. App. LEXIS 1360 (3rd Cir. NJ Jan. 23, 2009)

- 2 Level Sentence Enhancement for obstruction of investigation.
- 2 FBI agents Philadelphia field office
- Defendant's residence, inform suspect child porn
- Defendant admits, consents to search, shows agents to 2nd floor and computer, leave to 1st floor
- Return to computer, monitor message "Washing cache/cookies"
- Defendant reveals turning on computer activates an automatic software program that deletes temporary cached Internet files and cookies, unless manually bypassed.

United States v. Megahed, 2009 WL 722481 (M.D. Fla. March 18, 2009)

- Suspect not home FBI ask father for consent to search, FBI takes computer away August 6, 2007
- 2 months later father w/d consent, unclear when image made
- Computer not searched until a year later (apparently) key evidence discovered October 2008
- Motion to suppress evidence discovered – internet history file.
- After agents searched, seized computer, captured mirror image copy, and returned HD to defendant, evidence was discovered in course of examine of mirror image copy.
- In October 2008 neither defendant or his father retained a reasonable expectation of privacy in the mirror image copy.
- Valid consent to search carries the right to examine and photocopy.
  - See US v Ponder, 444 F. 2d 816, 818 (5th Cir. 1971): Mason v Pulliam, 557 F. 2d 426, 429 (5th Cir. 1977)(IRS document case).

United States v. Cotterman, 2009 U.S. Dist. LEXIS 14300 (DC Ariz. Feb. 23, 2009)

- Search only justified as a border search because no p/c at all to allow the search of the computer.
- Decision to search based upon a TECS hit out of California based upon the fact Defendant had a 15 year old child molestation conviction.
- Search could have been done, (while not necessarily to the convenience of the agents) at border, technician could have traveled from Tucson to do the analysis.
- Defendant and wife waited more than 8 hours at the border finally told computer going to be taken to Tucson even though he offered to help access the computer at the border. This offer was declined by the agents.
- Search took at least 48 hours to yield results.
- Cannot be said that Tucson became functional equivalent of border.
- Because Tucson not functional equivalent of border (170 miles away) Court agrees with the MJ evidence should be suppressed.

FTC v. Cyberspy Software, LLC, 2009 U.S. Dist LEXIS 13494 (M.D. Fla. Feb. 23, 2009)

- RemoteSpy
- Legitimate Use
- Substantial harm to consumers
- TRO enjoining sale

Becker, et al. v. Toca, 2008 U.S. Dist. LEXIS 89123 (E.D. La. Sept 26, 2008)

- Installed virus on office and personal computer to steal passwords
- Defendant motion to dismiss –
  - sending virus to detect and steal passwords located on a computer does not constitute an attempt to intercept and electronic communication for purposes of federal Wiretap act.
  - SCA does not apply
  - CFAA inapplicable – no harm plead
- Court held – Wiretap Act claim dismissed
- SCA claim unclear at this time whether Trojan program accessed information stored on device
- CFAA survives, harm sufficiently plead

Bailey v. Bailey, 2008 U.S. Dist. LEXIS 8565 (E.D. Mich. Feb. 6, 2008)

- **Key logger installed on computer shared by defendant and his ex-wife**
- **Wiretap Act Claim**
  - **No interception –**
    - **definition of "intercept" "encompasses only acquisitions contemporaneous with transmission." *United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003)*. See *Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994)*; *Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2001)*; *In re Pharmatrak, Inc., 329 F.3d 9 (1st Cir. 2003)*; and *Fraser v. Nationwide Mutual Ins. Co., 352 F.3d 107 (3rd Cir. 2003)*.**
- **SCA Claim**
  - **This court agrees with the reasoning in *Theofel*. The fact that Plaintiff may have already read the emails and messages copied by Defendant does not take them out of the purview of the Stored Communications Act. The plain language of the statute seems to include emails received by the intended recipient where they remain stored by an electronic communication service.**
  - **However, as a point of clarification, Stored Communications Act protection does not extend to emails and messages stored only on Plaintiff's personal computer. *In re Doubleclick Inc., 154 F. Supp. 2d 497, 511 (S.D.N.Y. 2001)*("the cookies' residence on plaintiffs' computers does not fall into *§ 2510(17)(B)* because plaintiffs are not 'electronic communication service' providers."). Defendant does not set forth any other basis for dismissing the claim. Accordingly, Defendant Bailey is not entitled to summary judgment on Plaintiff's [*18] claim for violation of *18 U.S.C. § 2701*.**

Responsible Disclosure

- **For the enterprise network manager, the notion of responsible disclosure has centered on the idea that major security flaws in products they use wouldn't be shared publicly in any way until a software vendor corrected them. That's the underlying premise of what's called the Organization for Internet Safety (OIS) guidelines first released five years ago and updated in 2004. An effort spearheaded by Microsoft, the OIS guidelines now face criticism from some of the very people who wrote them, who argue enterprises should know about serious flaws early for purposes of security workarounds.**
  - Ellen Messmer, Network World 5/31/2007

Responsible Disclosure

- **First Rule as Attorney – Never get near a Courtroom Especially in Criminal proceedings**
- **Recent Examples & Discussion**

Cyber Warfare & Definitions

Computer Network Security

Event Will Determine Response and Legal Authority

- **Multiple disciplines**
  - **Network Ops-CERTs/NOSCs**
  - **Intelligence**
  - **Counterintelligence**
  - **Law enforcement**
  - **Commander-in-Chief**
- **Computer Security**
  - **Events**
  - **Incidents**
  - **Intrusions**
  - **Attacks**

Calixte

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPREME JUDICIAL COURT
FOR SUFFOLK COUNTY
No. SJ-2009-0212

IN RE: MATTER OF A SEARCH WARRANT EXECUTED ON MARCH 30, 2009 AT THE RESIDENCE OF MOVANT RICCARDO CALIXTE

MEMORANDUM OF DECISION AND ORDER

Riccardo Calixte brings this petition pursuant to Mass. R. Crim. P. 15(a)(2), seeking the return of property that was seized pursuant to a search warrant issued by a clerk magistrate in the Newton District Court, and seeking relief from the denial, by a judge of that court, of his motion to quash the search warrant. The search warrant was for computer and other electronic equipment in Calixte's student residence at Boston College (BC). It was issued, executed and returned on March 30, 2009, and its execution resulted in the seizure of twenty-three items, including three laptops and various data storage devices. No criminal charges have yet resulted from the search. Calixte requests that the warrant be "quashed," that the property be returned, and that any evidence flowing from the search and seizure be suppressed.

Calixte

- College roommate domestic disturbance
- Roommate informs cops Calixte CS major
- Saw Hack into BC grading system
- 200+ illegally downloaded movies
- Seized – 3 laptops; 2 iPods; 2 cell phones; digital camera; numerous hard drives, flash drives, and compact disks.
- Commonwealth has begun to examine items seized but unable to access data on HD of Calixte's laptop
- Motion quash search warrant; return property; suppress any evidence from search in Newton District Court – Judge p/c exists, appeal

Gutman v Klein, 2008 U.S. dist LEXIS 92398 (E.D. N.Y. Oct. 15 2008) (Civil Litigation Case)

- **Spoliation of Evidence, deletion Defendant's laptop**
- **MJ ordered defendant to make available HDs, suspected tampering, MJ court appointed forensic expert examination**
- **“indicative of behavior of a user who was attempting to permanently delete selective files from the machine and then cover up the chronology of system changes occurring in the hours and days just prior to a forensic preservation."**
- **Litigation started 5 years earlier, duty to preserve, Defendant’s explanation contradictory and incredible.**
- **MJ what to do in response to spoliation – DJ**

Independent Newspaper, Inc. v. Brodie, 2009 Md. LEXIS (Ct. of Apps. Md. Feb 27, 2009)

- **When a trial court is confronted with a defamation action in which anonymous speakers or pseudonyms are involved, it should**
- **1 require plaintiff to undertake efforts to notify anonymous posters they are subject of a subpoena or application for an order of disclosure, including posting a message of notification of the identity discovery request on the message board;**
- **2 withhold action to afford the anonymous posters reasonable opportunity to file and serve opposition to the application;**
- **3 require plaintiff to identify and set forth exact statements purportedly made by each anonymous poster, alleged to constitute actionable speech;**
- **4 determine whether complaint has set forth a prima facie defamation per se or per quod action against the anonymous posters; and**
- **5 if all else is satisfied, balance anonymous poster's First Amendment right against *strength* of the *prima facie* case of defamation presented by plaintiff and necessity for disclosure of anonymous defendant's identity, prior to ordering disclosure.**

Computer Fraud and Abuse (CFAA) Cases

- ***Kluber Skahan & Associates, Inc. v. Cordogan, Clark & Assoc., Inc.*, 2009 U.S. Dist. LEXIS 14527 (N.D. Ill. February 25, 2009)**
- ***Motorola, Inc., v. Lemko Corp.*, 2009 U.S. Dist. LEXIS 10668 (N.D. Ill. February 11, 2009)**
- ***Lasco Foods, Inc., v. Hall and Shaw Sales*, 2009 U.S. Dist. LEXIS 4241 (E.D. Miss. January 22, 2009)**
- ***Condux International, Inc., v. Haugum*, 2008 U.S. Dist LEXIS 1000949 (D.Ct. Minn. December 15, 2008)**

Possession of Malware

- **Council of Europe's Convention on Cybercrime**
- **Federal U.S. law**
- **State law**
- **Possession of Burglary tools???**

Reverse Engineering

- **DMCA**
- **Supreme Court - Bonito Boats v. Thunder Craft Boats**
- **Sega Enterprise v. Accolade**
- **Atari v. Nintendo**
- **Sony v. Connectix Corp**

Contact Information

- robert.clark3@dhs.gov