

# **Legal Aspects of Cybersecurity**

---

**(AKA) Cyberlaw**

**A Year in Review**

**Cases & Issues**

**Your Questions**

**My (alleged) Answers**

Black hat USA  
August 4, 2011  
R.W. Clark



**Disclaimer**

# **Disclaimer - aka the fine print**

---

- **Joint Ethics Regulation**
- **Views are those of the speaker**
- **I'm here in personal capacity**
- **Don't represent view of government**
- **Disclaimer required at beginning of presentation.**

**All material - unclassified**

# **Legal Aspects of Cybersecurity**

---

**(AKA) Cyberlaw**

**Where Technology**

**And Law**

**Intersect**

# Agenda for Briefing

---

- **Special Skills**
- **Google & Wi-Fi**
- **Cybersecurity Legislation**
- **Lessons Learned –Cybersecurity**
- **Sony *et al***
  - **Geohot**
  - **Class Action & Negligence??**
- **Cases**
  - **Limitations on Searches of Computers**
  - **No Expectation Privacy/Exceeding Authority**
  - **Others**

# *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.**

# *Google and Wi-Fi*

---

- *In re Google Inc. Street View Electronic Communications Litigation*, --- F.Supp.2d ----, 2011 WL 2571632 (N.D.Cal. June 29, 2011)

# *Secure Your Wireless Router*

---

- ***United States v. Ahrndt*, 2010 U.S. Dist. LEXIS 7821 (D. Ore January 28, 2010)**
  - **Unsecured wireless router**
  - **Neighbor access**
  - **iTunes “share” library**
  - **Dad’s Limewire Tunes**



# *Secure Your Wireless Router*

---

- ***United States v. Ahrndt*, 2010 U.S. Dist. LEXIS 7821 (D. Ore January 28, 2010)**
  - Extent to which the *Fourth Amendment* provides protection for the contents of electronic communications in the Internet age is an open question. The recently minted standard of electronic communication via e-mails, text messages, and other means opens a new frontier in *Fourth Amendment* jurisprudence that has been little explored." *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 904 (9th Cir. 2008).
  - The issue in this case is whether the *Fourth Amendment* provides a reasonable, **subjective expectation of privacy** in the contents of a **shared iTunes library** on a personal computer connected to an **unsecured home wireless network**.

# *Secure Your Wireless Router*

---

- ***United States v. Ahrndt*, 2010 U.S. Dist. LEXIS 7821 (D. Ore January 28, 2010)**
  - **A *Fourth Amendment* search does *not* occur-even when the explicitly protected location of a house is concerned-unless 'the individual manifested a subjective expectation of privacy in the object of the challenged search,' and '**society is willing** to recognize that expectation as reasonable.'**"  
***Kyllo v. United States*, 533 U.S. 27, 33, 121 S. Ct. 2038, 150 L. Ed. 2d 94 (2001) [\*9] (quoting *California v. Ciraolo*, 476 U.S. 207, 211, 106 S. Ct. 1809, 90 L. Ed. 2d 210 (1986)).**

# *Secure Your Wireless Router*

## ■ *United States v. Ahrndt*, 2010 U.S. Dist. LEXIS 7821 (D. Ore January 28, 2010)

- Information transmitted to and from the internet is invisible to the other user of a Wi-Fi signal. Most **joyriders** assume that using another person's unsecured wireless connection is **entirely legal** and experts have pronounced it ethical. Randy Cohen, The Ethicist: Wi-Fi Fairness, **N. Y. Times**, Feb. 8, 2004, at 6, available at 2004 WLNR 5575601.
- In any event, **accidental unauthorized** use of other people's wireless networks is a fairly common occurrence in densely populated urban environments. Purposeful unauthorized use is perhaps equally **ubiquitous**, because, as one high-technology researcher put it, "Wi-Fi is in the air, and it is a very low curb, if you will, to step up and use it." Michel Marriott, Hey Neighbor. Stop Piggybacking on My Wireless, N.Y. Times, Mar. 5, 2006, at 11, available at 2006 WLNR 3698466.

# *Secure Your Wireless Router*

## ■ *United States v. Ahrndt*, 2010 U.S. Dist. LEXIS 7821 (D. Ore January 28, 2010)

- As a result of the ease and frequency with which people use others' wireless networks, I conclude that **society recognizes a lower expectation of privacy in information broadcast via an unsecured wireless network router** than in information transmitted through a hardwired network or password-protected network. Society's recognition of a lower expectation of privacy in unsecured wireless networks, however, does not alone eliminate defendant's right to privacy under the *Fourth Amendment*. In order to hold that defendant had no right to privacy, it is also **necessary** to find that **society would not recognize as reasonable an expectation of privacy in the contents of a shared iTunes library** available for streaming on an unsecured wireless network.

# *Latest Cases*

---

- *United States v. Hicks*
- *United States v. Fricosu*
- *United States v. Boucher (part duex)*

# *Cybersecurity Legislation*

---

## **Cybersecurity for .gov**

- **FISMA**

- **Authority with Executive Heads**
- **DHS in Support via MOA**

- **Proposed White House Legislation**

- **DHS in Charge**
- **Oversight Procedures**
- **CIP When Requested**
- **A Center/Protect Privacy ...**

# *Sony et al*

---

- **Sony Subpoenas**
  - **ISPs**
  - **Facebook**
  - **Twitter**
- **Class Action Negligence**

# *Negligence*

---

- **WSJ Tech Podcast 29 APR 2011**
  - **Former cyber prosecutor**
  - **Standard – Imperative duty**
  - **Not the standard**
- ***Shames-Yeakel v. Citizens Fin. Bank*, 677 F. Supp. 2d 994 (N.D. Ill August 21, 2009)**
- **Patco**



# *Sony Lawsuit*


---

- **Out of date Apache Servers**
- **No firewalls**
- **Dr. Spafford hearing House Subcommittee on Commerce**
- **Big company**
- **Easy to Update**
- **We'll get around to it ???**

# *Sony Lawsuit*

---

- **Negligence standard**
  - **RSA Breach**
  - **LastPass breach**
  - **HB Gary Breach**
  - **Etc....**



# *Cybersecurity Lessons Learned*

**Cases**

---

**From the**

**Past Year**

# *The Supreme Court*

---

- **Employer Monitoring**
- ***CITY OF ONTARIO, CALIFORNIA, ET AL. v. QUON***
  - **Banners**
  - **Training**
- **Patents**
- ***MICROSOFT CORP. v. I4I LIMITED PARTNERSHIP ET AL.***

# *Limitations On Searches of Computers*

---

- *In re United States' Application for a Search Warrant To Seize and Search Electronic Devices From Edward Cunniss, --- F.Supp.2d ----, 2011 WL 991405 (W.D.Wash., Feb 11, 2011)*

# *Limitations On Searches of Computers*

---

- ***United States v. Abdellatif*, --- F.Supp.2d ----, 2010 WL 5252852 (W.D.N.Y., Dec 16, 2010)**
  - **Searches of computers often involve a degree of intrusiveness much greater in quantity, if not different in kind, from other searches of containers; such considerations commonly support the need specifically to authorize the search of computers in a search warrant. Computers are capable of storing immense amounts of information and often contain a great deal of private information.**

# *Expectation of Privacy*

---

- *Shefts v. Petrakis*, --- F.Supp.2d ----, 2010 WL 5125739 (C.D. Ill. Dec 08, 2010)
- *United States v. Hamilton*, --- F.Supp.2d ----, 2011 WL 1366481 (E.D.Va. Apr 11, 2011)



# *Cases*

---

- *United States v. Nosal*
- *United States v. Cotterman*, 637 F.3d 1068, 2011 WL 1137302 (9th Cir. (Ariz.) Mar 30, 2011)
- *Juror Number One v. California*, 2011 WL 567356 (E.D.Cal., Feb 14, 2011)

# **Intrusion, Crime, . . .??**

---

- **Pursuant to 18 U.S.C. § 1030, 28 U.S.C. § 533, the FBI has primary investigative jurisdiction and is authorized to coordinate an intelligence, investigative, and operational response to major crimes within both state and federal jurisdictions.**

# **Intrusion, Crime, . . . ??**

---

- **US-CERT (DHS) 44 USC § 3546. Federal information security incident center**
  - (a) In general. The Director [of OMB] shall ensure the operation of a central Federal information security incident center to--**
    - (1) provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;**
    - (2) compile and analyze information about incidents that threaten information security;**
    - (3) inform operators of agency information systems about current and potential information security threats, and vulnerabilities**

# Intrusion, Crime, . . . ??

- US-CERT (DHS) HSPD 7, paragraph (16) The Secretary will continue to **maintain an organization** to serve as a **focal point** for the security of cyberspace. The organization will facilitate interactions and **collaborations** between and among Federal departments and agencies, State and local governments, the **private sector**, academia and international organizations. To the extent permitted by law, Federal departments and agencies with cyber expertise, including but not limited to the Departments of Justice, Commerce, the Treasury, Defense, Energy, and State, and the Central Intelligence Agency, will collaborate with and support the organization in accomplishing its mission. The organization's mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems. The organization will **support the Department of Justice and other law enforcement agencies** in their continuing missions to investigate and prosecute threats to and attacks against cyberspace, to the extent permitted by law

# Contact Information

---

- Are you kidding me