Legal Aspects of Cybersecurity – (AKA) CYBERLAW: A Year in Review, Cases, issues, your questions my (alleged) answers

The first responsibility of Government is to establish justice, insure domestic tranquility, provide for the common defense and secure the blessings of liberty to its people.[1] National security is safety from foreign coercion or intimidation.[2] This is the standard enshrined in international law by Article 2(4) of the United Nations charter as a prohibition against "the threat or use of force against the political independence or territorial integrity of any state."[3]

While there is no authoritative definition of "national security[4]" we recognize that our national security must consider our vital interests, critical interests, and peripheral interests. Vital interests are those that if lost directly endanger the security of the United States. Critical interests are those if lost would create a direct threat to one of our vital interests. Peripheral interests are those is lost would only distantly threaten a vital or critical interest.

The critical infrastructure of the United States is a vital resource and vital interest.[5] "Critical infrastructure" are systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters. There are 18 critical infrastructure sectors: agriculture and food; banking and finance; chemical; commercial facilities; commercial nuclear reactors, materials, and waste; communications; dams; defense industrial base; drinking water and water treatment systems; emergency services; energy; government facilities; information technology; national monuments and icons; postal and shipping; public health and health care; transportation systems; and critical manufacturing.[6]

In the past there have been major efforts both within and outside of government to protect United States information systems from hackers and other threats. These efforts might be categorized as efforts to: "harden" information systems by improving facilities, equipment, programming, procedures, and the training of administrators and authorized users; programs to deglamorize hacking and to educate the general public and potential hackers in the costs and other serious consequences of computer intrusions; and, measures to facilitate the identification and prosecution of offenders through law enforcement and criminal justice system.[7]

Many U.S. federal government departments and agencies have responsibilities and programs to address various aspects of cyber security. This level of federal effort demonstrates that cyber

---

[1] U.S. Const. preamble.
[2] John Norton Moore, *National Security Law* 3 (Carolina Academic Press 1990), p. 3 citing H.Lasswell, *National Security and Individual Freedom* 51 (1950, reprint 1971).
[3] John Norton Moore, *National Security Law* 3 (Carolina Academic Press 1990), p. 3.
[4] Phillip Johnson, A National Security Response to Computer Intrusions, p. 2 (September 8, 2000)(Draft for discussion only OASD(C3I))
[5] *See* National Strategy to Secure Cyberspace (2003) and GAO, *Cyber Analysis and Warning, DHS Faces Challenges in Establishing a Comprehensive National Capability*, GAO-08-588 (Washington, D.C. June 2008)(Draft Report)
[6] GAO, *Cyber Analysis and Warning, DHS Faces Challenges in Establishing a Comprehensive National Capability*, GAO-08-588 (Washington, D.C. June 2008)(Draft Report)
[7] Phillip Johnson, A National Security Response to Computer Intrusions, p. 2 (September 8, 2000)(Unpublished manuscript on file with the Asst. Sec. of Defense for C3I)

security is a national priority. However, critics claim that the many organizations and programs are unnecessarily duplicative and the Nation lacks a coherent strategy for understanding the true cyber security threat or the roles and responsibilities of each federal government organization.[8]

Cyber space means the interdependent network of information technology infrastructures.[9] The body of law and regulation that govern "cyber space" refer to it in terms of "computer network operations." Computer network operations have their foundations in statutes, legal precedents and several layers of implementing regulations issued by the federal government. These regulations clearly state that cyber security or computer network security is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.[10]

To accomplish this huge task computer network operations rely upon multiple disciplines within and outside of the federal government. Each one of these numerous organizations use their inherent capabilities and authorities to accomplish computer network operations and given the complexity of the global information grid, computer network operations requires close cooperation between network operations, intelligence, communications, counterintelligence and law enforcement communities. Moreover, the civilian/private counterparts operate in a remarkable similar fashion, they have CERTS/CIRTS and system administrators to act as first line defenders against unauthorized access and use.

To maneuver through this complicated process we call computer network operations requires a keen understanding of the multiple disciplines involved and the authorities and limitations each brings into CNO. This requires an understanding of two factors: first, one must understand the roles and responsibilities of each of the above identified disciplines; and, second, one must understand the basic foundations of the legal authorities used in CNO. The former requirement requires an analysis of the individual authorities that each discipline brings into CNO and a keen understanding of the limitations placed upon each of the disciplines. In other words, we must be extremely concerned with mission creep as it relates to computer network operations. Strict statutory construction,[11] as it is used by the Courts to interpret statutes, is helpful in understanding the roles and limitations of the various disciplines, operators, system administrators, law enforcement, counterintelligence, and intelligence. All the regulations that establish CNO identify these specific disciplines to assist in computer network security. They are named for a reason - - to adhere to existing laws and to avoid the previous abuses that

---

[8] John Rollins and Clay Wilson, Terrorist Capabilities for Cyberattack: Overview and Policy Issues, CRS Report for Congress p. 7 (January 22, 2007)

[9] Lieutenant Colonel Joshua E. Kastenberg, Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law, 64 A.F. L. REV. 43, p 48 (2009) *citing*, National Security Presidential Directive 54/Homeland Security Presidential Directive 23, "Cybersecurity Policy" (8 January 2008)

[10] Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy, ASD NII/DoD CIO, p. 1 (August 2009) found at, www.cio-nii.defense.gov/docs/DoD_IA_Strategic_Plan.pdf, *citing*, National Security Presidential Directive 54/Homeland Security Presidential Directive 23, "Cybersecurity Policy" (8 January 2008) *and* Shon Harris, CISSP All in One Certification Exam Guide, p. 62 - 64 (McGraw Hill 2002)

[11] Courts first look to the **plain meaning** of the terms of the statute in order to discern whether those terms impart sufficient clarity to a person of ordinary intelligence. *See United States v. Spy Factory*, 951 F. Supp. 450 (S.D. N.Y. 1997).

occurred in the name of domestic national security.[12] That means a lot of moving parts and much has been written already.[13] So why do I think I have anything to add to this? What could I add? Well, we will discuss that below.

First I would like to make what I think is a critical point for this entire area of full spectrum computer network operations. Words matter. As Catherine J.K. Sandoval, Assistant Professor of Law, Santa Clara University School of Law and Co-Director, Broadband Institute of California, stated in, Disclosure, Deception, and Deep-Packet Inspection: The Role of the Federal Trade Commission Act's Deceptive Conduct Prohibitions in the Net Neutrality Debate, 78 Fordham L. Rev. 641 (November 2009), "When I use a word," Humpty Dumpty said … "it means just what I choose it to mean – neither more nor less." (Citing Lewis Carroll, Through the Looking Glass 106 (Schocken Books 1987)(1872)).

Computer network operations involve events, incidents, intrusions, and attacks and those are responded to by numerous agencies using a multitude of differing authorities that will fall under computer network security; computer network defense; computer network exploitation; and/or, computer network attack. So because words and definitions do matter we need to stop calling everything that happens to someone's network or computer an attack. If everything is an attack, then nothing is an attack. And if everything is an attack then the Department of Defense needs to take charge since they are responsible for fighting and winning the country's wars.[14] Okay, I know I am being unrealistic. For example look at the story, "DNS Attack Briefly Takes Down E-Commerce Sites."[15] That's a lot sexier than, "DNS Intrusions Briefly Takes Down E-Commerce Sites." But words will matter when it comes to deciding who has primary jurisdiction over what computer network event, incident, intrusion, or yes, "attack."
And just as using the correct word is important so is using the correct authority. For many years

---

[12] *United States v. United States District Court for the Eastern District of Michigan, 407 U.S. 297 (1972)* (referred to as the *"Keith"* case).

[13] *See* Sean Condron, Getting It Right: Protecting American Critical Infrastructure in Cyberspace, 20 Harv. J. Law & Tec 404 (2007); Alan F. Williams, Prosecuting Website Development Under the Material Support to Terrorism Statutes: Time to Fix What's Broken, 11 N.Y.U. J. Legis. & Pub. Pol'y 365 (2007/2008); Thomas Wingfield, When is a Cyber Attack an Armed Attack, Potomac Institute for Policy Studies (February 2006); Todd M. Hinnen, The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet, 5 Colum. Sci. & Tech. L. Rev. 3 (2003/2004); Winston P. Nagan, The New Bush National Security Doctrine and the Rule of Law, 22 Berkeley J. Int'l L. 375 (2004); Eric Jensen, Unexpected Consequences From Knock-On Effects: A Different Standard for Computer Network Operations, 18 Am. U. Int'l Rev. 1145 (2003); Eric Jensen, Computer Attack on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense, 38 Stan. J. Int'l 207 (2002); Mary Ellen O'Connell, The Myth of Preemptive Self-Defense, The American Society of International Law: Task Force on Terrorism (August 2002); LTC Dhillon and LTC Smith, Defensive Information Operations and Domestic Law: Limitations on Government Investigative Techniques, 50 A.F. L. Rev. 135 (2001); William C. Banks, M.E. Bowman, Executive Authority for National Security Surveillance, 50 Am. U.L. Rev. 1 (October 2000); Roger D. Scott, Territorial Intrusive Intelligence Collection and International Law, 46 A.F. L. Rev. 217 (1999); Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, 37 Colum. J. Transnat'l L. 885 (1999); Todd A. Morth, Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter, 30 Case W. Res. J. Int'l L. 567 (Spring/Summer 1998); Roger Scott "Legal Aspects of Information Warfare: Military Disruption of Telecommunications, 45 Naval L. Rev. 57 (1998); *and,* Lawrence Greenberg, Information Warfare and International Law, National Defense University Press (1997).

[14] U.S. Dep't of Def., National Defense Strategy, p.6 (June 2008) *available at* http://www.defense.gov/news/2008%20National%20Defense%20Strategy.pdf.

[15] *See* http://gigalaw.blogspot.com/2009/12/dns-attack-briefly-takes-down-e.html (Source: CNN.com).

I have heard the cry for new legislation so various agencies could conduct a variety of "operations." While I realize there are global issues that need resolution, I am talking about the cries for new authorities that come from my tech colleagues. Remarkably, I believe all the legal authorities already exist necessary to accomplish full spectrum computer network operations. The challenge is not obtaining new legislation but rather identifying the correct organization or entity that has the right authority for the right action.

Curtis Karnow states, "The Internet, and its language of code, are global; they are not coterminous with any of the usual means of enforcement of laws and values, because the Internet is not coterminous with any country, region, or cultural group. The Internet gathers those who have no contractual relationship, no spoken language in common, and are not bound by a common law. Trade sanctions will not assist. Nations will not permit their citizens to be policed directly by authorities across the globe."[16]

Sean Condron captured this best, "Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.[17] In contrast, homeland defense is the protection of U.S. sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression, or other threats as directed by the President.[18] The Department of Homeland Security is the federal agency in charge of homeland security while the Department of Defense is the lead federal agency for homeland defense."[19]

To promote security, DHS was established to strengthen measures for protecting telecommunications and other critical infrastructure services; coordinate efforts to protect critical public and privately owned information systems within the United States from terrorist attack; coordinate efforts to ensure rapid restoration of telecommunications and other critical infrastructure facilities; and, coordinate efforts to ensure rapid restoration of public and private critical information systems.[20] Within the National Cyber Security Division of the Department of Homeland Security, the US-CERT serves as a focal point for addressing computer network security incidents within the federal government. One of the primary functions of the US-CERT is to increase the federal government's awareness of computer network threats and

---

[16] Curtis E.A. Karnow, Launch on Warning: Aggressive Defense of Computer Systems, 9 Int'l J. Comm. L. & Pol'y 4 (Fall 2004)

[17] Sean Condron, Getting it Right: Protecting American Critical Infrastructure in Cyberspace, 20 Harv. J. Law & Tec 404, p 404 (Spring 2007) citing *6 U.S.C.A. § 111*(b)(1)(A)-(C) (West 2002); *see also* THE PRESIDENT OF THE UNITED STATES, NATIONAL STRATEGY FOR HOMELAND SECURITY 30 (2002) [hereinafter HOMELAND SECURITY], *available at* http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf. Homeland Security Presidential Directive 7 suggests an expansion of critical infrastructure sectors when it assigns roles and responsibilities of sector-specific federal agencies. *See* PRESIDENT OF THE UNITED STATES, HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 7 (2003), *available at* http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

[18] Sean Condron, Getting it Right: Protecting American Critical Infrastructure in Cyberspace, 20 Harv. J. Law & Tec 404, p 404 (Spring 2007) citing 42 U.S. DEP'T OF DEF., STRATEGY FOR HOMELAND DEFENSE AND CIVIL SUPPORT 5 (2005) [hereinafter HOMELAND DEFENSE], *available at* http://www.defenselink.mil/news/Jun2005/d20050630homeland.pdf.

[19] Sean Condron, Getting it Right: Protecting American Critical Infrastructure in Cyberspace, 20 Harv. J. Law & Tec 404, p 404 (Spring 2007)(Citations omitted).

[20] Exec. Order 13228, "Establishing the Office of Homeland Security and the Homeland Security Council," 66 Fed. Reg. 51812 (Oct. 8, 2001); 6 U.S.C. §§ 101 *et seq.*

vulnerabilities thereby increasing the government's ability to prepare for and respond to computer network security events. The US-CERT is the Federal government's computer network security organization responsible for increasing the security of federal systems.

The main three principles of security are confidentiality, integrity and availability.[21] Confidentiality provides the ability to ensure that the necessary level of security is enforced at each junction of data processing and prevention of unauthorized disclosure.[22] Integrity is upheld when the assurance of accuracy and reliability of information and systems is provided, and unauthorized modification of data is prevented.[23] Availability is that the systems and networks should provide adequate capacity in order to perform in a predictable manner with the acceptable level of performance.[24]

Cyberspace means the interdependent network of information technology infrastructures.[25] "Cybersecurity or computer network security is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation."[26] "Computer network defense is the mission to defend computer systems and networks from unauthorized activity and other activity, which degrade mission performance and adversely impact survivability."[27] This mission is to be accomplished by using communications, law enforcement, counterintelligence, and intelligence community capabilities in response to specific or potential threats.[28] The inclusion of defense against potential threats is another clear statement of the United States commitment to apply anticipatory self-defense in the area of CNO."[29]

---

[21] 44 U.S.C. § 3542(b)(1)(A-C) and *see* Shon Harris, CISSP All in One Certification Exam Guide, p. 62 (McGraw Hill 2002)

[22]Shon Harris, CISSP All in One Certification Exam Guide, p. 63 (McGraw Hill 2002)

[23]Shon Harris, CISSP All in One Certification Exam Guide, p. 63 (McGraw Hill 2002)

[24] Shon Harris, CISSP All in One Certification Exam Guide, p. 64 (McGraw Hill 2002)

[25] Statement for the Record Lieutenant General Keith Alexander, Commander Joint Functional Component Command for Network Warfare, Before the House Armed Services Committee Terrorism, Unconventional Threats, and Capabilities Subcommittee (5 May 2009) *citing* Deputy Secretary of Defense Memorandum, Subject: *The Definition of Cyberspace*, May 12, 2008 (The Department of Defense holds this definition is consistent with the definition of cyberspace provided in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), which states that cyberspace is "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.). Found at *http://armedservices.house.gov/pdfs/TUTC050509/Alexander_Testimony050509.pdf*

[26] Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy, ASD NII/DoD CIO, p. 1 (August 2009) found at, www.cio-nii.defense.gov/docs/DoD_IA_Strategic_Plan.pdf , *citing*, National Security Presidential Directive 54/Homeland Security Presidential Directive 23, "Cybersecurity Policy" (8 January 2008)

[27] Eric Talbot Jensen, Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense *38 Stan. J Int'l L. 207*, fn 138 (Summer, 2002)

[28] Eric Talbot Jensen, Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense *38 Stan. J Int'l L. 207*, fn 138 (Summer, 2002).

[29] Eric Talbot Jensen, Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense *38 Stan. J Int'l L. 207*, fn 138 (Summer, 2002).

Computer network exploitations are enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.[30] Computer network attack is action taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.[31]

There are several definitions used to explain access that occurs on a computer network system.

-Security event - an occurrence in a system that is relevant to the security of the system. The term covers both events that are security incidents and those that are not.[32]
-Security incident – (1) a security event that involves a security violation, in other words, a security event in which the system's security policy is disobeyed or otherwise breached; (2) any adverse event that compromises some aspect of computer or network security; (3) a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.[33]
-Security intrusion – a security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so.[34]
-Attack – (1) An intentional act by which an entity attempts to evade security services and violate the security policy of a system. That is, an actual assault on system security that derives from an intelligent threat; (2) a method or technique used in an assault.[35]

[30] Joint Chiefs of Staff, Joint Pub. 1-02, Department of Defense Dictionary of Military and Related Terms 203 (12 Apr 2001).
[31] Joint Chiefs of Staff, Joint Pub. 1-02, Department of Defense Dictionary of Military and Related Terms 203 (12 Apr 2001).
[32] R. Shirey, Internet Security Glossary, Version 2, Request For Comments 4949, p. 268 (The IETF Trust, August 2007) at http://www.rfc-editor.org/rfc/rfc4949.txt and NIST SP 800-61 and NIST SP 800-61 Computer Security Incident Handling Guide (Draft) July 2008.
[33] R. Shirey, Internet Security Glossary, Version 2, Request For Comments 4949, p. 269 (The IETF Trust, August 2007) at http://www.rfc-editor.org/rfc/rfc4949.txt.
[34] R. Shirey, Internet Security Glossary, Version 2, Request For Comments 4949, p. 269 (The IETF Trust, August 2007) at http://www.rfc-editor.org/rfc/rfc4949.txt.
[35] R. Shirey, Internet Security Glossary, Version 2, Request For Comments 4949, p. 21 (The IETF Trust, August 2007) at http://www.rfc-editor.org/rfc/rfc4949.txt.

Precedents in Cybersecurity and Cases from the past year.

United States v Prochner, 417 F.3d 54 (1st Cir. 2005)

Special Skill Enhancement

Defendant appeals from his sentence on a conviction of access device (credit card) fraud. He pled guilty to knowingly possessing fifteen or more unauthorized credit card numbers with the intent to defraud in violation of *18 U.S.C. § 1029(a)(3)*. District court sentenced him to 25 months in prison and three years of supervised release, and ordered restitution in the amount of $2,610.19. The sentence was based in part on enhancements for the amount of loss, number of victims, special skill, and obstruction of justice. Defendant challenges the enhancement for use of a special skill.

On August 20, 2002, Prochner was trying to enter Canada from New York when Canadian law enforcement officers conducting border inspections discovered that he was carrying papers and a notebook containing numerous credit card numbers. Further investigation revealed that the credit card numbers had been reported as stolen or lost and that fraudulent activity had been reported on the accounts. After being advised of his rights, Prochner admitted that he had obtained the credit card numbers on the Internet. In a written statement to law enforcement, he explained that he accessed website order logs to obtain the credit card numbers and then accessed channels where he determined that the numbers were still valid.

In addition to the credit card numbers, Prochner had in his possession a handwritten journal that included references to adolescent males.

Sentencing

The presentence report (PSR) determined that Prochner's base offense level was 6; added 4 levels for the loss of $ 17,000 ($ 500 multiplied by 34 credit card numbers); 2 levels for the number of victims (between 10 and 50); **2 levels for the use of a special skill**; and, 2 levels for obstruction of justice. The resulting offense level totaled 16. Defendant had no prior convictions and zero criminal history points, he was assigned to Criminal History Category I. The resulting guideline sentencing range was 21 to 27 months. The Probation Office calculated that Prochner owed $ 2,610.19 in restitution.

Special Skill Enhancement

Prochner contends the court erred in finding that, to facilitate the offense, he used a "special skill," as defined in sentencing guidelines, to obtain the credit card numbers.

The Guidelines direct that a two-level enhancement is applied "if the defendant . . . used a special skill, in a manner that significantly facilitated the commission or concealment of the offense." A "special skill" is defined as "a skill not possessed by members of the general public and usually requiring substantial education, training or licensing." Examples include "pilots, lawyers, doctors, accountants, chemists, and demolition experts.

We have held that a defendant need not necessarily have formal education or training in order to be found to possess a special skill. *Montero-Montero*, 370 F.3d at 123; *United States v. Nelson-Rodriguez*, 319 F.3d 12, 58 (1st Cir. 2003); *United States v. Noah*, 130 F.3d 490, 500 (1st Cir. 1997). A special skill may also be acquired through experience or self-tutelage. *Noah*, 130 F.3d at 500 (finding that a self-taught, professional tax preparer utilized a special skill in preparing and electronically filing tax returns).

The district court adopted the PSR's conclusion that Prochner "used self-taught computer skills to 'hack' into website order logs." Prochner argues, however, that there is no evidence that he has education or training (even self-taught) in computers. But a court can reasonably infer requisite self-education from the nature and extent of the skill possessed. Here, **Prochner's own description** of what he did and could do to hack into secure websites and purloin data revealed a high and unusual level of computer know-how. The court could infer that this came from self-tutelage and experience if not from more formal training.

In his written statement to law enforcement at the time he was arrested, Prochner explained how he had obtained the credit card numbers:

> After accessing the internet, via telnet and MIRC/PIRCH and accessing websites' order logs via Cart32 (internet credit card ordering programs), I scanned twenty some credit cards . . . . Credit cards can be checked for validity via bots (i.e., scripts that check cards are still active/inactive), and I used a (MIRC) based program via Windows 98SE, on an Undernet channel and a Dalnet based channel to check three or four AMEX cards and found them to be "extremely" valid.

Prochner went on to elaborate on what he called "carding," including how websites use SSL encryption, how one can rewrite the websites' "cgi scripts" which ultimately hold the "logs" for credit card orders for a particular website, and how one can download an international chat client to access thousands of channels where one can check the validity of all kinds of credit card numbers. He stated that these channels are "where the true criminals are." Prochner went on to explain that "[he] can easily access these places [at] any computer [at] any time of the day, via a Windows Based program." He also claimed that "even without log orders or hacking (for lack of a better word) tools, a novice Internet surfer can access these channels and still get hundreds of credit cards in less than 2 [hours]."

A skill can be special even though the activity to which the skill is applied is mundane." Id. The critical question is "whether the defendant's skill set elevates him to a level of knowledge and proficiency that eclipses that possessed by the general public. *Noah*, 130 F.3d at 500.

Prochner's description of the processes to obtain the credit card numbers amply supports the district court's conclusion that Prochner's special skills, including the ability to "hack" into website order logs and computer networks and to re-write "cgi scripts," exceed the knowledge of the average Internet user. Even without expert evidence, Prochner's affidavit supports finding a level of sophistication well beyond the ordinary. We are unable to say, therefore, that the district court's determination that Prochner possessed a special skill not possessed by members of the general public is clearly erroneous.

Wi-Fi

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

Plaintiffs bring this putative class action against Google alleging three causes of action for violation of the federal Wiretap Act, violation of Cal. Bus. & Prof.Code §§ 17200, *et seq.*, and violation of various state wiretap statutes. Plaintiffs allege that Defendant intentionally intercepted data packets, including payload data, from Plaintiffs' Wi–Fi networks utilizing specially designed packet sniffer software installed on Defendant's Google Street View vehicles.

Before the Court is Defendant's Motion to Dismiss. The Court dismisses the state wiretap claims as preempted by the Federal wiretap Act. But the other two causes of action move forward.

Google alleged to have Google Street View vehicles equipped with nine directional cameras to capture 360 degree views of the streets and 3G/GSM/Wi–Fi antennas with custom-designed software for the capture and storage of wireless signals and data. The data collection system is commonly known as a packet analyzer, wireless sniffer, network analyzer, packet sniffer or protocol analyzer.

The matter before the Court presents a case of first impression as to whether the Wiretap Act imposes liability upon a defendant who allegedly intentionally intercepts data packets from a wireless home network.

Plaintiff's complaint alleges that Google intentionally intercepted electronic communications sent or received on wireless internet connections. Based on the allegations above, the Court finds that Plaintiffs plead facts sufficient to state a claim for violation of the Wiretap Act. In particular, Plaintiffs plead that Defendant intentionally created, approved of, and installed specially-designed software and technology into its Google Street View vehicles and used this technology to intercept Plaintiffs' data packets, arguably electronic communications, from Plaintiffs' personal Wi–Fi networks. Further, Plaintiffs plead that the data packets were transmitted over Wi–Fi networks that were configured such that the packets were not readable by the general public without the use of sophisticated packet sniffer technology. Although Plaintiffs fail to plead that the wireless networks fall into at least one of the five enumerated exceptions to Section 2510(16)'s definition of "readily accessible to the general public" for radio communications, the Court finds that the wireless networks were not readily accessible to the general public as defined by the particular communication system at issue, wireless internet networks, which are not "radio communications," as the term was intended by Congress in drafting Section 2510(16).

Rather, application of the Section 2510(16) definition of "readily accessible to the general public" as narrowly defined for traditional radio broadcast technology, would be inapplicable to the determination of whether Plaintiffs' allegedly intercepted data packets from their Wi–Fi networks are readily accessible to the general public for purposes of exemption G1, despite the fact that wireless networks transmit data using radio waves. As the Court has found, Congress intended Section 2510(16)'s definition to resolve the issue of radio scanning devices used to

intercept radio broadcasts by establishing a presumption that traditional radio services were "readily accessible to the general public," in accord with the design of the medium as one where most communications over that medium are intended to be public. **Unlike in the traditional radio services context, communications sent via Wi–Fi technology, as pleaded by Plaintiffs, are not designed or intended to be public. Rather, as alleged, Wi–Fi technology shares a common design with cellular phone technology, in that they both use radio waves to transmit communications, however they are both designed to send communications privately, as in solely to select recipients, and both types of technology are architected in order to make intentional monitoring by third parties difficult. S.Rep. No. 99–541, at 6 (1986). (Emphasis added.)**

Further, applying Section 2510(16)'s narrow definition of "readily accessible to the general public" to wireless networks, a technology unknown to the 99th Congress who drafted and passed the ECPA, would contravene the primary stated purpose of the amendment, which was to update the Wiretap Act to include within the Act specific protections against intentional interceptions of computer-to-computer communications and so-called "electronic mail" or email; data Plaintiffs plead was included in the data packets intercepted by Defendant. Interpreting the ECPA such that the statute provides obscure limitations on the protection of emails and other computer-to-computer communications based on the particular medium that transmitted the electronic communication would render the Wiretap Act, and the efforts of the 99th Congress to provide such protections, absurd. Under such an interpretation, the Act would provide a private civil right of action, and even impose criminal liability, for the interception of emails transmitted over an ethernet cable through a wired network, but would stop short at protecting those very same emails should they pass momentarily over radio waves through a Wi–Fi network established to transmit data within a home.

Defendant's contention that Plaintiffs fail to state a claim for violation of the Wiretap Act, as Plaintiffs plead that their networks were "open" and "unencrypted," is misplaced. While Plaintiffs plead that their networks, or electronic communications systems, were configured such that the general public may join the network and readily transmit electronic communications across that network to the Internet, Plaintiffs plead that the networks were themselves configured to render the data packets, or electronic communications, unreadable and inaccessible without the use of rare packet sniffing software; technology allegedly outside the purview of the general public. Thus, the Court finds that Plaintiffs plead facts sufficient to support a claim that the Wi–Fi networks were not "readily accessible to the general public," such that exemption G1 would not apply.

Defendant's interpretation of *United States v. Ahrndt* as standing for the principle that all unencrypted wireless networks are readily accessible to the general public and, thus, any interceptions from those networks are obviated from liability under exemption G1, unduly extends the doctrine. (Motion at 10–11.) In *Ahrndt*, a neighbor was connected to the Internet via her own wireless network when her network malfunctioned and her computer automatically logged in to another open wireless network operated by the defendant. *Id.* at 1. The defendant had administered his iTunes software as set to "share," such that other users on the same network would be able to access all files that the defendant had stored in his iTunes libraries. *Id.* After being automatically logged into the defendant's wireless network, the plaintiff in *Ahrndt* began

using her own iTunes program and noticed that the defendant's iTunes library was accessible. *Id.* In accessing the defendant's iTunes library, the plaintiff located a number of files containing child pornography in a subfolder within the shared directory. *Id.* Based on these facts, Judge King held that the plaintiff's interception was not illegal and was, in fact, "expressly lawful" under the Wiretap Act as the defendant's network and iTunes software were configured to be readily accessible to the general public. *Id.* at 8. However, the court did not base its holding merely on the fact the defendant's network was unencrypted. *Id.* Rather, Judge King found that "defendant's conduct in operating his iTunes software with the preferences set to share, in conjunction with maintaining an unsecured wireless network router, diminished his reasonable expectation of privacy to the point that society would not recognize it as reasonable." *Id.* at 8. Unlike in *Ahrndt,* here, Plaintiffs plead that, although the networks themselves were unencrypted, the networks were configured to prevent the general public from gaining access to the data packets without the assistance of sophisticated technology. Thus, the Court finds that, without more, merely pleading that a network is unencrypted does not render that network readily accessible to the general public and serve to remove the intentional interception of electronic communications from that network from liability under the ECPA.

United States v. Ahrndt, 2010 WL 373994 (D.Or. Jan 28, 2010)

Before the court is defendant's Motion to Suppress, which seeks to suppress evidence defendant alleges was obtained as a result of an illegal search in violation of his constitutional rights under the *Fourth Amendment*. For the following reasons, I deny defendant's motion.

Defendant's neighbor erroneously connects to his open and unencrypted Wi-Fi, SSID Belkin54G, and observes files with child pornography names. Neighbor contacts LEA.

In order to benefit from *Fourth Amendment* protections, an individual must demonstrate a subjective expectation that his activities would be private, and he must show that his expectation was one that society is prepared to recognize as reasonable." *U.S. v. Young*, 573 F.3d 711, 715-16 (9th Cir. 2009) (internal citations omitted). Evidence seized in violation of the *Fourth Amendment* constitutes an illegal search or seizure. See *Pennsylvania Bd. of Prob. and Parole v. Scott*, 524 U.S. 357, 362, 118 S. Ct. 2014, 141 L. Ed. 2d 344 (1998). Evidence seized during an illegal search is tainted and should not be included in the affidavit for a search warrant. Inclusion of tainted evidence in the affidavit though, does not in itself taint the warrant or evidence seized pursuant to it. The court should excise the tainted evidence and decide if the remaining, untainted evidence provides probable cause to issue a warrant. *United States v. Bishop*, 264 F.3d 919, 924 (9th Cir. 2001). Furthermore, to be untainted by the prior illegal search, the officer's decision to seek the warrant must not have been prompted by what he saw during the prior illegal search. *United States v. Hill*, 55 F.3d 479, 481 (9th Cir. 1995).

"The 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.

Defendant argues that when Officer McCullough duplicated the steps taken by JH and viewed defendant's child pornography, he conducted an illegal warrantless search in violation of defendant's *Fourth Amendment* right to privacy. According to Defendant, a warrantless search occurred because the facts indicate Officer McCullough's violated his reasonable expectation of privacy in his computer files. Alternatively, defendant argues that his expectation of privacy was per se reasonable because JH's conduct was illegal under the Electronic Communications Privacy Act. Defendant contends that all information gathered subsequently was fruit of the poisonous tree and thus inadmissible. The government disagrees with defendant's contentions, maintaining that defendant's conduct in operating his home computer system eliminated his right to privacy.

"[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)(quoting *California v. Ciraolo*, 476 U.S. 207, 211, 106 S. Ct. 1809, 90 L. Ed. 2d 210 (1986)).

Defendant argues that a wireless network should be given no less protection than a hardwired network under the *Fourth Amendment*. Courts, however, have long held that different communications hardware and technologies carry different reasonable expectations of privacy. The expectation of privacy in cordless phones is analogous to the expectation of privacy in wireless networks, because wireless networks are so easily intercepted. **Wireless networks are similar to cordless phones in that they transmit data over radio waves.** James Ridge, What Happens When Everything Becomes Connected: The Impact on Privacy When Technology Becomes Pervasive, *49 S. Tex. L. Rev. 725, 735 (2008)*. Unlike cordless phone signals, however, a wireless router signal can be received by an unauthorized user even though that user will not usually encounter personal or confidential information. Daniel Kamitaki, Beyond E-mail: Threats to Network Security and Privileged Information for the Modern Law Firm, *15 S. Cal. Interdisc. L.J. 307, 340 (2006)*. By using the wireless network signal for internet access, a joyrider is not made privy to personal information of the broadcasting user. Ned Snow, The Law of Computer Trespass: Cyber Security or Virtual Entrapment?, 2007 Ark. L. Notes 109, 110 (2007). Information transmitted to and from the internet is invisible to the other user of a Wi-Fi signal. Id. In addition, most joyriders assume that using another person's unsecured wireless connection is entirely legal, *Kamitaki, supra at 340-41*, 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. *Kamitaki, supra at 341*. 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.

Here, defendant used a Belkin54G wireless router to blanket his house and the surrounding area with wireless internet. He did not password-protect the wireless network, so any person within range could access it. Neighbors had accessed the Belkin54G router multiple times. At the hearing, special agent Tony Onstadt testified that although the default setting of the Belkin54G router is not to have password protection, the router comes with a manual that includes detailed instructions on how to password-protect the router. According to his testimony, the manual stresses the importance of password protection. Agent Onstadt also testified that the range of the router was up to 400 feet in the shape of a donut around the house.

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.

As a general matter an individual has an objectively reasonable expectation of privacy in his personal computer. *United States v. Heckenkamp,* 482 F.3d 1142, 1146 (9th Cir. 2007). The expectation of privacy in the information on one's computer, however, can be diminished by one's conduct with the computer. See *United States v. Ganoe,* 538 F.3d 1117, 1127 (2008). For example, when a person uses peer-to-peer file sharing software to download child pornography from others, but fails to configure his computer not to share his own files, he "open[s] up his download folder to the world, including [police]." If the individual "kn[ows] or should [know] that the software [installed on the computer] might allow others to access his computer," he lack[s] a reasonable expectation of privacy in the files stored on his computer."

Ahrndt used LimeWire, to download the child pornography in this case. The folder that JH and Officer McCullough viewed was called "Dad's LimeWire Tunes" because LimeWire has the capability to integrate with iTunes and automatically places all downloaded material in a LimeWire playlist in the iTunes library. Nevertheless, the child pornography in this case was discovered via the iTunes software, not the LimeWire software.

Defendant's argument and analogy, however, ignore certain key facts and misunderstand crucial technological details. Defendant was not merely using his unsecured wireless network. He was also using his iTunes software, and its preferences were set to actively share his music, movies, and pictures with anyone who had access to the same wireless network.

The iTunes software is a robust, multipurpose music and video management software with many capabilities. Users are able to share iTunes content over networks, within which each user can access another user's files. Within a network, a user can listen to another user's music or view another's movies or images, but he cannot download files from another user. Id. Special agent James Cole testified that the default setting of iTunes is *not* to share music or images. Agent Cole's testimony is confirmed by the Apple support website, which lists six affirmative steps a user must take in the software's preferences in order to enable sharing. iTunes:

When a person shares files on LimeWire, it is like leaving one's documents in a box marked "free" on a busy city street. When a person shares files on iTunes over an unsecured wireless network, it is like leaving one's documents in a box marked "take a look" at the end of a cul-de-sac. I conclude that iTunes' lesser reach and limit on file distribution does not render it unlike LimeWire in terms of its user's reasonable expectation of privacy.

United States v. Beatty, 2009 U.S. Dist. LEXIS 121473 (W.D. Penn Dec 31, 2009)

Here, the Government contends that the Defendant has no reasonable expectation of privacy in the files retrieved from his computer, at least to the extent the files were located in a shared folder. The Government cites *United States v. Stults*, 575 F.3d 834, 843 (8th Cir. 2009), *United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir 2008); *United States v. Perrine*, 518 F.3d 1196, 1205 (10th Cir. 2008); *United States v. Barrows*, 481 F.3d 1246, 1249 (10th Cir. 2007); *United States v. Brese*, 2008 U.S. Dist. LEXIS 28916, 2008 WL 1376269, at 2 (W.D. Okla. 2008); *United States v. Borowy*, 577 F. Supp. 2d 1133, 1136 (D. Nev. 2008); and *United States v. Meysenburg*, 2009 U.S. Dist. LEXIS 34619, 2009 WL 1090664 (D. Neb. 2009), as supporting the proposition that an individual using peer-to-peer software to share files on his computer cannot claim the protection of the *Fourth Amendment* relative to those shared files.
The Government's argument would have more force if the Defendant were challenging Trooper Pearson's use of P2P software to remotely access his shared files, but that is not the situation here. As the Defendant points out, the cases cited by the Government generally recognize that law enforcement officers do not violate the *Fourth Amendment* by using P2P software to remotely access files contained on a defendant's computer that are being shared by the defendant inasmuch as the defendant has no reasonable expectation of privacy regarding the remote accessing of those files. *See Stults*, 575 F.3d at 843

Subpoena Powers & Discovery

Sony v George Hotz
A federal magistrate grants Sony’s request for information from PayPal account of George Hotz. Two weeks earlier Magistrate Joseph Spero in San Francisco granted Sony the right to acquire the internet IP addresses of anybody who had visited Hotz’s website from January of 2009 onward.

Negligence

Shames-Yeakel v. Citizens Fin. Bank, 677 F. Supp. 2d 994 (N.D. Ill. Aug 21, 2009)

CFAA

United States v. Nosal, 2010 WL 934257 (N.D. Cal. Jan 6, 2010)

Employee exceeds authorized access when he or she violates the employer’s computer access restrictions, including use restrictions.

Lee v. PMSI, Inc., 2011 WL 1742028 (M.D. Fla. 2011)

United States v. Rodriguez, 628 F.3d 1258 (11th Cir. Dec 27, 2010)

Technology

United States v. Kramer, 2011 U.S. App. Lexis 2367 (W.D. Missouri Feb 8, 2011)

Defendant's cellular telephone was a "computer" under Sentencing Guideline.

ECPA

Shefts v. Petrakis, --- F.Supp.2d ----, 2010 WL 5125739 (C.D. Ill. Dec 08, 2010)

Company computer, laptop, and handheld device, and interception of his communications on these devices violated Federal Wire and ECPA, the Stored Communications Act (SCA), the Computer Fraud and Abuse Act (CFAA), and the Illinois Eavesdropping Statute.

Company president's text messages were intercepted, for purposes of ECPA at point when company's spyware acquired and logged the messages but president consented to interception of his e-mail correspondence.

Mortensen v Bresnan Communications, L.L. C, 2010 WL 5140454 (D. Mont. Dec 13, 2010)

Bowers v. Kletke, 2010 U.S. Dist. LEXIS 104435 (W.D. Wash. Sept 29, 2010),

Grey v. Kirkland & Ellis, 2010 U.S. Dist. LEXIS 91726 (N.D. Ill. Sept 2, 2010)

United States v. Szymuszkiewicz, 2010 U.S. App. LEXIS 18815 (7th Cir. Sept 9, 2010)

Defendant charged with intercepting supervisor's e-mail messages and he claimed that the evidence was insufficient to support a conviction. Court affirmed. Other employees testified that defendant was sophisticated about computers and that it was common knowledge as to how to set up a forwarding rule. Defendant acquired the e-mails by using at least three devices, and he accessed nonpublic messages by means of a device capable of understanding them but unnecessary to the communication itself.

Fourth Amendment & Searches

United States v. Padilla, 2011 WL 2110305 (S.D. Miss., May 25, 2011)

Pornography was found on a laptop computer following a roadside search of Padilla's vehicl the search at the county barn, and the search of Padilla's computer were all fruit of the poiso the initial roadside search of the vehicle. The vehicle was relocated to the county barn with his written consent to search the computer was tainted and is not valid.
United States v. Flowers, 2011 WL 1664440 (5th Cir. (Tex.) May 02, 2011)

Flowers challenges officers' protective sweep of his house after they executed his arrest warrant,

the warrantless, consensual search of his house and computer thereafter, and the voluntariness of statements that he made to law enforcement. The district court did not clearly err in determining that Flowers voluntarily consented to the search of his home and computer. In evaluating the voluntariness of Flowers's consent, this court considers six factors.

People v. Stipo, 2d Crim. No. B218512, (Ct Apps of Cal, 2nd Dt, Div 6 May 16, 2011)

Conviction and sentencing of defendant for computer hacking-related offenses are upheld where defendant lacks standing to challenge a search warrant served on an Internet Service Provider (ISP) because an internet service subscriber has no expectation of privacy in the subscriber information he supplies to the ISP.

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)

Search warrant application overbroad and violated the Fourth Amendment

United States v. Hamilton, --- F.Supp.2d ----, 2011 WL 1366481 (E.D.Va. Apr 11, 2011)

Defendant, public school employee, lacked objectively reasonable expectation of privacy, for Fourth Amendment purposes, in e-mails between him and his wife that were stored on his work computer, since, at time search warrant for his work computer was executed, he was on long-standing notice that contents of his computer were subject to inspection; although the e-mails were exchanged prior to defendant's employer's adoption of computer use policy, employer subsequently adopted computer use and privacy policy providing that all information created, sent, received, or stored in employer's computer system was subject to inspection and monitoring at any time as authorized by Superintendent or designee, and forms acknowledging policy were electronically signed in defendant's name on his computer

United States v. Cotterman, 637 F.3d 1068 (9th Cir. (Ariz.) Mar 30, 2011)

In a dispute involving the scope of the border search doctrine, judgment by the district court that the search of property seized at an international border and moved 170 miles inland for further search cannot be justified by the border search doctrine is reversed where neither the scope of the intrusion nor the duration of the deprivation was egregious.

United States v Whaley, 2011 WL 521174 (11th Cir. (Fla.) Feb 16, 2011)

Officer had probable cause to seize computer for further investigation and defendant knowingly and voluntarily consented to search of computer, any delay in searching hard drive did not unreasonably interfere with defendant's possessory interest.

United States v. Muhlenbruch, --- F.3d ----, 2011 WL 536493 (8th Cir. (Iowa), Feb 17, 2011)

Private citizen's search of defendant's apartment did not implicate defendant's Fourth Amendment rights; defendant's consent to search of his home computer and files contained

therein was voluntary

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.

United States v. Trainor, 2011 WL 250431 (D.N.D., Jan 26, 2011)

United States v. Stabile, --- F.3d ----, 2011 WL 294036 (3rd Cir. (N.J.) Feb 01, 2011)

Scope of the plain view doctrine in the context of computer search.

United States v. Krupa, --- F.3d ----, 2011 WL 353212 (9th Cir. (Cal.), Feb 07, 2011)

United States v. Szymanski, --- F.3d ----, 2011 WL 350294, 6th Cir. (Ohio), Feb 07, 2011)

United States v. Warshak, --- F.3d ----, 2010 WL 5071766, 6th Cir. (Ohio), Dec 14, 2010)

Work Place Searches

United States v. Hamilton, --- F.Supp.2d ----, 2011 WL 1366481 (E.D.Va. Apr 11, 2011)

Blogging

Juror Number One v. California, 2011 WL 567356 (E.D.Cal. Feb 14, 2011)

Plaintiff Juror Number One was the jury foreperson in a trial in Sacramento County Superior Court. During the criminal trial, plaintiff posted certain comments on his Facebook page stating that he was "still" on jury duty. Once, he stated that he was "bored" during the presentation of cell phone record evidence. One of the other jurors in the criminal trial, Juror Number Five, became "friends" with plaintiff on Facebook. The jury reached a guilty verdict in the criminal trial on June 25, 2010. Afterward, Juror Number Five contacted defense counsel and stated that plaintiff had posted "comments about the evidence during trial" on his Facebook page.

Trademarks

Network Automation, Inc., v. Advance Systems Concepts, Inc.,

In a trademark infringement dispute involving whether the use of a trademarked name by defendant to advertise its products through search engine searches is a violation of the Lanham Act, 15 U.S.C. section 1114, injunctive relief by district court in favor of plaintiff is reversed where plaintiff failed to show likelihood of confusion.

Lahoti v. Vericheck, Inc.,

In a trademark and cyberlaw case, the district court's finding on remand, that appellant violated the Lanham Act, the Anticybersquatting Consumer Protection Act (ACPA), the Washington Consumer Protection Act (WCPA), and Washington common law, is affirmed where the district court followed this court's instructions in finding that defendant Vericheck, Inc.'s VERICHECK mark is suggestive, and thus entitled to trademark protection.

JustMed, Inc. v. Byce, 2010 U.S. App. LEXIS 6976 (9th Cir. April 14, 2009)

A dispute arose over whether plaintiff, a small technology start-up company, owned the source code developed for its product. The district court did not err in holding that defendant was an employee and that the source code was a work made for hire; the contemplated indefinite duration of the relationship, the tasks defendant did for the company, the fact that defendant earned a salary from the company, and the nature of the company's business all support the finding that defendant was an employee. The company's failure to comply with federal and state employment or tax laws was more likely attributable to the start-up nature of the business than to defendant's alleged status as an independent contractor.

Return of Property Damage to Property

In re Grand Jury, __ F.3d __, 2011 WL 522942 (3rd Cir. 2011).