NEW YORK UNIVERSITY

INTELLECTUAL PROPERTY AND ENTERTAINMENT LAW LEDGER

VOLUME 1 SPRING 2010 NUMBER 2

SOFTWARE DEVELOPERS, ON GUARD!: OFFERING SOFTWARE FOR SALE CAN TRIGGER A BAR TO PATENTABILITY EVEN IF THE SOFTWARE IS UNTESTED AND INCOMPLETE

PAUL A. RAGUSA AND JACK CHEN*

Paul A. Ragusa and Jack Chen discuss the on-sale bar to patentability in the context of nascent software. They conclude that a simple investigation concerning whether software code was complete at the time of an offer for sale is insufficient to establish the critical date for the purposes under 35 U.S.C. § 102(b) ("Conditions for patentability").

In *Pfaff v. Wells Elecs., Inc.*,[1] the Supreme Court formulated the now well known test for determining when an invention cannot be patented due to a sale or offer for sale more than one year prior to the filing of a patent application. Specifically, the Court held that an invention need not be "reduced to practice" at the time of the sale or offer to create a statutory bar against patent protection.[2] Instead, a sale or offer of an invention "ready for patenting," is sufficient to raise a statutory bar.[3] The purpose of the on-sale bar is to encourage early disclosure of inventions to the public as well as to prevent a de facto patent

* Paul A. Ragusa is a partner and Jack Chen an associate in the New York office of Baker Botts LLP, where they practice intellectual property law with an emphasis on patent litigation, patent portfolio management, counseling, and licensing.

[1] 525 U.S. 55 (1998).

[2] *Id.* at 67.

[3] *Id.* at 68.

term extension by those who would commercially exploit an invention for an extended period of time prior to filing a patent.

During the past twelve years, the courts have applied the *Pfaff* test to various technologies, some with more clarity than others. One thorny area involves the application of the *Pfaff* test in the context of software related inventions. Although the *Pfaff* Court rejected precedent that an invention needed to be "substantially complete" to provide a statutory bar,[4] it did not address how a software related invention can be ready for patenting where the code is incomplete, and untested. As a practical matter, how is a court to determine whether an unfinished software-related invention is ready for patenting and therefore can operate to trigger an on-sale bar? A recent district court decision addresses this issue head-on and is discussed below.

I. BACKGROUND

An applicant may be barred from patenting a software method after offering it for sale even if the computer code implementing the method is incomplete at the time of the offer. The patent statute states, "[a] person shall be entitled to a patent unless…the invention was…on sale in this country, more than one year prior to the date of the application for patent in the United States."[5] The purpose of the on-sale bar is to encourage early disclosure and to prevent inventors from removing existing knowledge from public use.[6]

The on-sale bar applies when two conditions are met: (i) the invention is the subject of a commercial offer for sale and (ii) the invention is ready for patenting prior to the statutory one-year period.[7] An invention is "ready for patenting" where either (i) the invention has been reduced to practice or (ii) the inventor had prepared drawings or other descriptions of the invention that were sufficiently specific to enable a person skilled in the art to practice the invention.[8]

II. ROBOTIC VISION SYSTEMS

The Court of Appeals for the Federal Circuit addressed the *Pfaff* test in the context of an invention involving software or computer programming in*Robotic Vision Sys., Inc. v. View Eng'g, Inc.*[9] There, the court addressed a software method

[4] *Id.* at 66.
[5] 35 U.S.C. § 102(b).
[6] *Pfaff*, 525 U.S. at 64.
[7] *Id.* at 67-68.
[8] *Id.* at 68.
[9] 249 F.3d 1307, 1312 n.2 (Fed. Cir. 2001).

for scanning leads on integrated circuit devices. The application for Robotic's patent was filed on June 24, 1992, establishing a one-year date of June 24, 1991.[10] In March of 1991, Robotic sold one of its scanning devices to Intel Corporation and agreed to deliver the patented device to Intel by June 3, 1991, thereby establishing a commercial offer for sale in March 1991, prior to the critical date of June 24, 1991.[11]

The Federal Circuit determined whether the claimed invention was ready for patenting prior to the critical date. Some time between March and April of 1991, a co-inventor of the patented scanning method, William Yonescu, disclosed the claimed method to Daniel Briceno of Robotic and asked him to write the software to implement the method.[12] It was undisputed that Briceno ultimately completed the software program according to Yonescu's description in March-April 1991, thereby establishing that Yonescu's description was sufficiently specific to allow Briceno to practice the invention and that the claimed invention was ready for patenting prior to the critical date of June 24, 1991.[13]

According to the court, the second *Pfaff* requirement may be satisfied even though there is no "actual completion of such software…, provided that there is a disclosure that is sufficiently specific to enable a person skilled in the art to write the necessary source code to implement the claimed method."[14] Under the *Pfaff* test, Robotic's invention was therefore invalid due to an on-sale bar.[15]

III. NETSCAPE COMMC'NS CORP.

Netscape Commc'ns Corp. v. ValueClick, Inc.[16] involved the cookies feature of the popular Netscape browser in which a piece of data, called a "cookie" and stored on the user's local computer, could be sent to the remote web server to enable the remote server to remember previous interactions with the user. For example, a remote server could identify a particular user by his or her cookie and present the user with his or her stored shopping cart of merchandise.

ValueClick argued that the cookie feature was the subject of an offer for sale as early as July or August of 1994, more than one year prior to the filing of the

[10] *Id.* at 1309.
[11] *Id.* at 1311.
[12] *Id.*
[13] *Id.* at 1311-12.
[14] *Id.* at 1312 n.2.
[15] *Id.* at 1312-13.
[16] No. 1:09cv225, 2010 U.S. Dist. Lexis 8733 (E.D. Va 2010).

corresponding patent application on October 6, 1995.[17] Netscape countered that no software product could have included the cookie feature prior to the one-year date (October 6, 1994) because the public release of the Netscape browser did not occur until after that date (October 13, 1994). Thus, Netscape argued that the cookie feature was not reduced to practice prior to the on-sale bar date.[18]

According to the District Court, "this statement misunderstands the law governing the 'ready for patenting' Pfaff prong because it assumes that an invention is only reduced to practice, and thus the on-sale bar can only be applied, after the source code has been perfected."[19] Testimony by Netscape's expert revealed that a draft version of source code pertaining to the cookie feature was entered into Netscape's software repository on October 4, 1994.[20] Netscape also testified that part of the method was completed by October 6, 1994, and that an early version of the code was entered into the software repository on October 3, 1994.[21] Thus, the District Court concluded that the existence of the draft source code prior to October 6, 1994, although perhaps incomplete, demonstrated that the method was ready for patenting prior to the critical date.

The court went further. "Moreover, with respect to inventions involving computer code, Pfaff simply requires complete conception of the invention, not the source code's actual completion, provided that there is an enabling disclosure that would allow one skilled in the art to complete the invention."[22] In a declaration to the Patent and Trademark Office, Netscape's Chief Technology Officer, John Giannandrea, stated that Netscape's software developer, Lou Montulli, disclosed the cookie invention, which corresponded to claim 1 of the patent-in-suit, during design review meetings in July and August of 1994.[23] According to Giannandrea, the meetings involved Giannandrea and Montulli drawing the software architecture for the cookie invention on a white board.[24]

The District Court found that Giannandrea, a software developer with more years of experience than Montulli, was a person of ordinary skill in the art for purposes of the *Robotic* test.[25] The July/August disclosure to Giannandrea and

---

[17] *Id.* at 8779-80.
[18] *Id.* at 8779.
[19] *Id.* at 8780.
[20] *Id.* at 8779.
[21] *Id.*
[22] *Id.* at 8780 (citing *Robotic Vision Sys.*, 249 F.3d at 1311-13).
[23] *Id.* at 8745-8746 n.8, 8782-83.
[24] *Id.* at 8782-83.
[25] *Id.* at 8782.

Montulli's completion of the source code in October of 1994, coupled with Giannandrea's years of software programming experience, constituted an enabling disclosure that would have enabled Giannandrea to write the source code. Accordingly, the District Court held that the evidence showed that the cookies invention was "ready for patenting" under the second prong of the *Pfaff* test.

IV. CONCLUSION

The *Netscape* case highlights the risk of offering for sale software products that are under development. A simple investigation concerning whether software code was complete is insufficient to establish the critical date for the purposes of § 102(b). Instead, an investigation should determine when the invention was disclosed in sufficient detail to enable one of ordinary skill in the art to write software, regardless of the state of software development.

USING CLEAN HANDS TO JUSTIFY UNCLEAN HANDS: HOW THE EMERGENCY EXCEPTION PROVISION OF THE SCA MISAPPLIES AN ALREADY CONTROVERSIAL DOCTRINE

BRENDAN J. COFFMAN*

While the government's encouragement—and even reliance—on third-party monitoring of citizens is not a new phenomenon, the emergency exception to the SCA adopted in the Patriot Act oversteps constitutional bounds by providing the executive with the incentive to exaggerate potential threats in order to gain the collaboration of the telecommunications companies. The policies underlying this strategy are similar to those explained and adapted by the Sixth Circuit while articulating its Clean Hands Exception. Brendan Coffman argues that by allowing the government to gain access to evidence it normally would not be able to obtain, and ignoring the normal parameters of the exclusionary rule, the Sixth Circuit created a regime encouraging complicity between law enforcement and private citizens. Similarly, the arguments running contrary to the Clean Hands Exception ring true when assessing the emergency exception: the government has too great an incentive to encourage third parties to violate the privacy rights of others, and the third parties, especially telecommunications companies, are ultimately trapped in a Hobson's Choice.

INTRODUCTION

A man sits in his apartment in a major United States city checking his email. He may or may not be a U.S. citizen, and may or may not be associated with a significant international organization. The government's intelligence agencies are not aware of the man, and local police officials have no overt reason to suspect anything abnormal or threatening. His email is transmitted and stored by a major electronic communications service provider, and his private messages on the server contain information vital to his plot—to attack a major U.S. city.

In the adjacent apartment, a man sends an email to a friend discussing his desire—mostly imaginary, but frighteningly realistic—of assaulting his female neighbor. The friend's wife intercepts the email. The wife does not believe the man

* Brendan Coffman is a student at the George Mason University School of Law, class of 2011, and alumnus of Georgetown University's Walsh School of Foreign Service. He is an Articles Editor of the George Mason Law Review.

would follow through on his desires, and goads him on in response. Much like the case above, the police have no reason to suspect any dangerous intention from this man.

In a third apartment lives a naturalized man originally of Arab citizenry. He is a stand-up citizen, but a local police officer distrusts the man, and suspects the man of plotting an attack. The police officer has no information to justify this premonition, and cannot effectuate a warrant. But he believes that if he had access to the man's email and other electronic communications, he could prove his suspicions.

Each man's email is stored with an internet service provider ("ISP"). In which of these circumstances could the ISP choose to voluntarily violate the privacy of one of the men and provide the government with the information contained within his email communications? In which of these circumstances should the ISP choose to disclose the information? Furthermore, when must the ISP disclose this information? Lastly, what does this mean in terms of Fourth Amendment privacy rights and the authority of law enforcement professionals?

The government's encouragement—and even reliance—on third-party monitoring of citizens is not a new phenomenon. As technologies have continued to advance, and telecommunications companies have expanded their sphere of influence over the day-to-day operations of citizens' lives, a natural partnership has arisen between the government and the telecommunications industry.[1] But 9/11 and the subsequent War on Terror[2] have introduced a new level of urgency to the government's need for information,[3] thus straining the relationship between the government and telecommunications companies.[4] While telecommunications companies often seek to help the government for both patriotic and commercial

[1] Jamie S. Gorelick et al., *Navigating Communications Regulation in the Wake of 9/11*, 57 Fed. Comm. L.J. 351, 353 (2005).

[2] President George H. Bush, Address to Congress (September 21, 2001).

[3] Access to information is the government's foremost necessity with respect to prevention of terrorist attacks. There is an inherent tradeoff of personal liberties when the government augments its need and collection of information. As a result, government involvement with information collection, particularly electronic surveillance, breeds a great deal of resentment, distrust, and skepticism from the public. S*ee, e.g.*, Wayne McCormack, Understanding the Law of Terrorism 203-212 (2008) (explaining the government's dilemma with respect to gathering intelligence in hopes of preventing an attack and cultivating distrust among the public); Allison M. Buxton, *In re Sealed Case: Security and the Culture of Distrust*, 29 Okla. City U. L. Rev. 917, 929-31 (2004) (explaining the American public's cultural distrust of law enforcement and surveillance activities generally).

[4] Gorelick, *supra* note 1, at 353.

reasons, the fear of lawsuits[5] and customer outrage requires them to pursue a more tempered approach to disclosure of customer information.

Congress passed the Stored Communications Act ("SCA")[6] in 1986 to limit electronic communications service providers' ability to disclose private information, and regulate the government's ability to compel these disclosures[7] The SCA requires the government to follow specified legal procedures to access private communications.[8] These procedures become increasingly more burdensome for the government as the information it seeks is more private and protected.[9] The SCA also contains a recently amended provision governing the voluntary disclosure of private information by Providers in the case of an emergency.[10] The emergency exception allows the Provider to disclose the contents of a customer's communication "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency."[11]

The "clean hands" exception allows the government to introduce evidence into trial that was illegally obtained by a third party when the government did not play any role in obtaining that information.[12] The clean hands exception stands in contrast to the exclusionary rule in that it values the state's interest in prosecuting the defendant more than the defendant's right to privacy.[13] It is vital to remember that the clean hands exception only applies in incidents in which the government played no part in the obtaining of the information.[14] While the very existence of the

---

[5] Under the amended language, communications provider who discloses records or other information pursuant to authorization contained in 18 U.S.C. § 2702(c)(4) in emergency circumstances has same protection from lawsuits as provider who discloses records pursuant to court order. *See* In re Application of U.S. For a Nunc Pro Tunc Order For Disclosure of Telecomms. Records, 352 F. Supp. 2d 45 (D. Mass. 2005).

[6] 18 U.S.C. §§ 2701-2712 (1986) (last amended 2008).

[7] Seth Rosenbloom, *Crying Wolf in the Digital Age: Voluntary Disclosure Under the Stored Communications Act*, 39 Colum. Hum. Rts. L. Rev. 529, 531-32 (2008).

[8] *Id.*

[9] *Id.*

[10] 18 U.S.C. § 2702(b)(8) (2006).

[11] *Id.*; § 2702(c)(4) (2001).

[12] *See infra* Part II.A.

[13] Shaun T. Olsen, *Reading between the Lines: Why a Qualified "Clean Hands" Exception Should Preclude Suppression of Wiretap Evidence under Title III of the Omnibus Crime Control and Safe Streets Act of 1968*, 36 Val. U. L. Rev. 719, 745-46 (2002).

[14] *Id.*

"clean hands" exception has split federal circuits,[15] Congress never clarified its legislative intent. However, the rationale underlying the clean hands exception is present in Congressional amendments to the SCA. This Comment argues that although amendments to the voluntary disclosure provisions of the SCA are ostensibly an update and ratification of previously existing standards for the controversial 'clean hands' exception, the SCA's emergency exception extends the rationale far beyond the boundaries of the clean hands exception. This difference is markedly different from the "lucky break" fortuitous logic implicated within the clean hands exception.[16]

This Comment begins with a primer on the laws regulating third party surveillance and its intersection with government access to information obtained by a third party. Part I provides an overview of the Fourth Amendment, its application to electronic surveillance, and a discussion of the exclusionary rule governing the admissibility of evidence obtained in violation of the Fourth Amendment. Part I then assesses the Sixth Circuit's clean hands exception, including an explanation of the rationale underlying the exception and a discussion of the primary cases invoking the doctrine. Part I next addresses the inadequacies of the Fourth Amendment right to privacy and exclusionary rule pertaining to its application to electronic information as a result of the business records cases. Part I concludes with an overview of Congressional response to these inadequacies through the enactment of several privacy-driven statutes, most notably the Stored Communications Act,[17] with particular focus on the compulsory, voluntary, and emergency disclosure provisions aimed at the telecommunications industry in 18 U.S.C. §§ 2702 and 2703.

Part II examines connections between the clean hands exception and the amended portions of the SCA. Secondly, Part II conducts an analysis of the deterring factors facing ISPs in each instance, and concludes that the modified voluntary disclosure provisions in Section 2702(b)(8) are less constrained than its clean hands counterpart because of the lack of a legitimate scheme to deter abuses. Part II concludes with a forecast of some of the difficulties that may arise in applying the SCA as a result of these similarities, and argues that the potential for encouraged abuses of the voluntary disclosure provisions may overextend the

[15] The Sixth Circuit stands alone in its application of the clean hands exception to Title III third party surveillance and has been rebuked by several other Circuits. *Compare* United States v. Murdock, 63 F.3d 1391 (6th Cir. 1995) *with* United States v. Crabtree, 565 F.3d 887 (4th Cir. 2009).

[16] *See infra* Part D.2.

[17] 18 U.S.C. §§ 2701-2712 (1986).

SCA's application. Finally, Part III demonstrates this vulnerability through an application of SCA and clean hands exception logic to the hypothetical scenarios presented at the onset of this Comment.

I. BACKGROUND

A. Stored Communications and Internet Service Providers

The growth and pervasion of the internet in the day-to-day lives of Americans cannot be overstated.[18] In the 10 years between 1997 and 2007, the percentage of American households containing computers with internet access has grown from 18% to 61.7%.[19] The ability to communicate across the internet, particularly though e-mail, has been a major factor in the growth of the internet.[20]

The structure of the internet, and the fact that we communicate through its unique structure, has a significant effect on both the Fourth Amendment privacy protections of these communications as well as the subsequent regulation of the internet communication industry.[21] Individuals using the internet do not communicate directly with another person. Instead, they transmit data across a network and through an ISP, who then routes the data to the desired endpoint.[22] This voluntarily disclosure of information to a third party invokes a body of controversial Fourth Amendment law.[23]

Internet communication is further complicated by another unique aspect of electronic communications. ISP's generally store records of all communications passing through their servers.[24] This further distinguishes e-mail from telephonic conversations, in which the communications company merely transmits the

---

[18] *See* Pew Internet & American Life Project, Daily Internet Activities, 2000-2009, *available at*http://www.pewinternet.org/Static-Pages/Trend-Data/Daily-Internet-Activities-20002009.aspx (showing that over 50% of American adults use the internet every day, and that almost 50% send or receive email every day).

[19] United States Census Bureau, Current Population Survey Reports, October 2007, http://www.census.gov/population/www/socdemo/computer.html (last visited April 15, 2010).

[20] K. G. Coffman & A. M. Odlyzko, *Growth of the Internet,* AT&T Labs Research, July 6, 2001, *available at* http://www.dtc.umn.edu/~odlyzko/doc/oft.internet.growth.pdf (last visited April 15, 2010).

[21] Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It,* 72 Geo. Wash. L. Rev. 1208, 1209-10 (2004).

[22] *Id.*

[23] *See infra* Part I.B.

[24] Alexander Scolnik, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment,* 78 Fordham L. Rev. 349, 359 (2009) (explaining ISPs' protocol for storing transactional communication information on their servers).

information over their line. ISPs often utilize the communications in the emails passing through their servers to accumulate information about the tendencies and profiles of their customers, as well as to protect their network from any harm that might be caused by customers.[25]

B. The Fourth Amendment and Protection of Personal Privacy

The Fourth Amendment demands that all searches and seizures be reasonable. The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[26]

The Fourth Amendment represents the Founders' belief that personal privacy was fundamental to the success of the American polity.[27] Some commentators have posited that the Fourth Amendment's protection of privacy rights is America's "most prized possession"[28] and the element of the Constitution that most directly affects and influences the lives of Americans.[29] The Fourth Amendment's Warrant Clause, including the requirement that a judge authorize a police officer's determination of probable cause, provides a substantial check on the Executive's ability to interfere with the personal privacy rights of the citizens during the course of criminal investigation.[30] However, the application of the

---

[25] *Id.*

[26] U.S. Const. amend. IV.

[27] William B. Cuddihy & B. Carmon Hardy, *A Man's House Was Not His Castle: Origins of the Fourth Amendment to the United States Constitution*, 37 Wm. & Mary Q. 372, 400 (1980). Cuddihy and Hardy argue that the Fourth Amendment "represented an American extension of the English tradition that a man' house was his castle…[t]he requirement that all search warrants be specific, the heart of the Fourth Amendment, accordingly enlarged the tradition's scope, for it controlled searches by the government to a degree never previously attempted." *Id.*

[28] Marjorie G. Fribourg, The Bill of Rights: Its Impact on the American People 10 (1967) (explaining that the protection of personal rights is the most fundamental distinguishing factor in America's Constitution).

[29] William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 Am. U. L. Rev. 1, 2-4 (2001).

[30] Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083, 1126 (2002) (explaining James Madison's belief that the structure of the Constitution and the insertion of the judicial branch in the middle of the executive branch's investigative process would lead to the best solution).

Fourth Amendment to surveillance, and particularly electronic surveillance, is not as clear.[31]

1. The Exclusionary Rule, Evidence Suppression, and the Good Faith Exception

Concerns over individual privacy complications in electronic surveillance have their roots in the Fourth Amendment exclusionary rule, which has been used to deter police officers from engaging in unconstitutional searches.[32] The exclusionary rule excludes or suppresses evidence obtained in violation of an accused person's constitutional rights.[33] For example, under the exclusionary rule, if police conduct a search without a warrant or probable cause, or obtain a warrant through misinformation, and evidence obtained by the search is suppressed.[34] The exclusionary rule applies in both state and federal courts.[35] While some argue that this rule is a disservice to the criminal justice system, it is one of the most fundamental deterrents to illegal search and seizure in the American criminal justice system.[36]

---

[31] Banks & Bowman, *supra* note 29, at 3-4; David Hardin, *The Fuss over Two Small Words: The Unconstitutionality of the USA PATRIOT Act Amendments to FISA Under the Fourth Amendment*, 71 Geo. Wash. L. Rev. 291, 295-97(2003) (explaining that finding space for electronic surveillance in the Fourth Amendment doctrine has been difficult); James X. Dempsey; *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 Alb. L.J. Sci. & Tech. 65, 69-71 (1997) (explaining that the indiscriminate nature of electronic surveillance has posed greater threats to privacy than physical search and seizure).

[32] Rosenbloom, *supra* note 7, at 537.

[33] Black's Law Dictionary 1464 (8th ed. 2004). Many commentators debate the merits of the exclusionary rule, arguing that it creates an unfair position for the government in having to both combat crime and uphold civil liberties. For a discussion focusing on the dilemmas in applying the exclusionary rule. *See*, Randy E. Barnett, *Resolving the Dilemma of the Exclusionary Rule: An Application of Restitutive Principles of Justice*, 32 Emory L.J. 937 (1983).

[34] *See, e.g.*, *Wong Sun v. United States*, 371 U.S. 471 (1973).

[35] Weeks v. United States, 232 U.S. 383 (1914). *Weeks* remains the landmark case in the creation of the exclusionary rule in federal courts, whereas Mapp v. Ohio extended the rule to state courts. 367 U.S. 643 (1961).

[36] *See, e.g.*, *Mapp*, 367 U.S. at 648; Lawrence Crocker, *Can the Exclusionary Rule Be Saved?*, 84 J. Crim. L. & Criminology 310, 310-14 (1993). Many substitutions for the exclusionary rule have been suggested, most notably a solution in which violating police officers are liable in damages to individuals whom they arrest with the aid of illegally obtained information. *See* Pierre Schlag, *Assaults on the Exclusionary Rule: Good Faith Limitations and Damage Remedies*, 73 J. Crim. L. & Criminology 875 (1982).

The Supreme Court introduced an important exception to the exclusionary rule in *United States v. Leon*: the "good faith" exception.[37] In *Leon*, the Court held that when police officers discovered evidence while acting on a defectively administered warrant the evidence from trial because the officers' reliance on the correct administration of the warrant had been made in objectively reasonable good faith.[38] The Court reasoned that that the exclusionary rule is designed to deter police officers, as opposed to a magistrate who issues a warrant.[39] The Court then concluded that excluding the evidence in this case would not serve the purpose behind the exclusionary rule.[40] As a result, a balancing test has evolved to determine the application of the exclusionary rule in the instance of a good faith police error in which the court considers the nature and intent of the Fourth Amendment violation against the applicability and necessity of tangible evidence.[41]

The *Leon* court enumerated four instances in which the good faith exception will not apply to avoid suppression of evidence through the exclusionary rule. First, the good faith exception does not apply if police officers provide misleading or untrue information to a magistrate.[42] Secondly, the good faith exception does not apply if law enforcement officials have reason to know that a magistrate has "wholly abandoned his judicial role."[43] Thirdly, the good faith exception does not apply if a warrant is completely unsatisfying of the probable cause standard to the extent that a reasonable police officer should know it is invalid.[44] Lastly, the good faith exception will not apply if the warrant is facially defective.[45] This rule and series of exceptions reinforces the notion that the Fourth Amendment prohibition of unreasonable search and seizure is at its heart a balancing test.[46]

---

[37] United States v. Leon, 468 U.S. 897 (1984).

[38] *Id.* at 918.

[39] *Id.*

[40] *Id.*

[41] *Id.* at 908-913.

[42] *Id.* at 922-23 (citing Franks v. Delaware, 438 U.S. 154 (1978)).

[43] *Id.* at 23 (citing Lo-Ji Sales, Inc. v. New York, 442 U.S. 319 (1979) (warrant at issue "left it entirely to discretion of officials conducting search to decide items which were likely obscene and to accomplish seizure").

[44] *Leon*, 468 U.S. at 922 (quoting Brown v. Illinois, 422 U.S. 590 (1975) (Powell, J., concurring)).

[45] *Id.*; 1 Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment § 1.3 (4th ed. 2004).

[46] *See, e.g.*, Donald Dripps, *The Case for the Contingent Exclusionary Rule*, 38 Am. Crim. L. Rev. 1, 2 (2001) (arguing that the Supreme Court has appeared to "have adopted *both* positions" in the debate over the exclusionary rule).

2. The Fourth Amendment and Electronic Communications

Historically, the Executive Branch asserted its right to conduct warrantless searches of electronic communications in both the domestic and national arenas as part of its task to protect national security.[47] Some have argued that the Founders simply did not contemplate the possibility of electronic communications, and as such, Fourth Amendment privacy concerns should be limited to criminal investigations and not applied to civil litigation.[48] Initially, the Executive faced very little resistance in its broad application of Executive authority in electronic surveillance due to the 1928 Supreme Court decision *Olmstead v. United States*.[49] In *Olmstead*, police wiretapped defendant's phone without a warrant because they suspected he was violating the National Prohibition Act.[50] The *Olmstead* court interpreted the Fourth Amendment's privacy protection very narrowly and very literally, holding that its protections extended only to physical searches and seizures.[51] Since the police did not detain the defendant, enter his home in any manner, or seize any of his material objects, the court held that the police did not violate the Fourth Amendment.[52]

The limited scope of constitutional privacy protections set forth in *Olmstead* suffered gradual erosions between 1928 and 1967, albeit outside the

---

[47] David Hardin, *The Fuss over Two Small Words: The Unconstitutionality of the USA PATRIOT Act Amendments to FISA Under the Fourth Amendment*, 71 Geo. Wash. L. Rev. 291, 296-97 (2003).

[48] Banks & Bowman, *supra* note 29, at 3-4. Banks and Bowman explain "Moreover, the Fourth Amendment was designed to protect against overreaching in investigations of criminal enterprises. Investigations of politically motivated threats to our national security, such as terrorism or espionage, were simply not contemplated." *Id.* Prior to the enactment of the 14th Amendment, the Supreme Court suggested that warrants issued pursuant to federal civil litigation may not be protected by the Fourth Amendment. *See* Murray's Lessee v. Hoboken Land & Improvement Co., 59 U.S. 272, 285 (1855). However, after the enactment of the 14th Amendment, the Supreme Court clarified its previous holding and narrowed its decision strictly to due process. *See* Walker v. Sauvinet, 92 U.S. 90, 92-93 (1875); Pac. Mut. Life Ins. Co. v. Haslip, 499 U.S. 1, 30-32 (1991) (explaining the interplay between *Murray's Lessee* and *Walker*).

[49] Olmstead v. United States, 277 U.S. 438 (1928).

[50] *Id.* at 455-57.

[51] *Id.* at 457.

[52] *Id.* at 466. Justice Brandeis' dissent foreshadowed the short lifespan of the *Olmstead* decision. Brandeis proclaimed "[The Founders] conferred, as against the Government, the right to be left alone – the most comprehensive of rights and the right most valued by civilized men. To protect, that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment." *Id*. at 478.

arena of electronic surveillance.[53] However, it was not until 1967 when the Supreme Court, in two landmark decisions, set the standard for individual privacy protection in the face of government electronic surveillance. First, in the June 1967 decision *Berger v. New York*,[54] the Court declared unconstitutional a New York statute that permitted law enforcement to engage in wiretapping based merely on the reasonable ground that the wiretap may obtain evidence of an unspecified crime.[55] The Court held that the New York statute lacked the "requirement for particularity in the warrant as to what specific crime has been or is being committed" and reversed defendant's conviction.[56]

The *Berger* Court included a dissent from Justice White that foreshadowed the uncomfortable intersection between electronic surveillance for the purposes of law enforcement and surveillance in the name of national security.[57] Justice White attached an appendix to his opinion entitled "Excerpt from 'The Challenge of Crime in a Free Society,' A Report by the President's Commission on Law Enforcement and Administration of Justice, at 200-203 (1967)."[58] The excerpt highlights the numerous difficulties experienced by the executive in administering surveillances, and calls upon Congress to "enact legislation dealing specifically with wiretapping and bugging."[59] Notably, the Commission Report suggested "All private use of electronic surveillance should be placed under rigid control, or it

---

[53] Several Supreme Court cases advanced the scope of the Fourth Amendment's privacy protections. The Court's first recognition of a Constitutional right to privacy concerned the freedom to associate. *See* NAACP v. Alabama ex rel. Patterson, 357 U.S. 449, 466 (1958) (holding that a private association could not be forced to disclose the names of its members). The Court also found constitutionally protected right to political privacy in Watkins v. United States, 354 U.S. 178 (1957) and Sweezy v. New Hampshire, 354 U.S. 234 (1957). The most important case to advance the privacy rights of individuals during this time period was Griswold v. Connecticut, 381 U.S. 479 (1965) (holding that a Connecticut law criminalizing the use of contraceptives violated a constitutional right to marital privacy and was therefore unconstitutional). This summary was adapted from Banks & Bowman, *supra* note 29, at 44-47.

[54] 388 U.S. 41.

[55] *Id.* at 63-64. The *Berger* court was extremely divided and contained three vociferous dissents from Justice Black, Justice Harlan, and Justice White. *Id.* at 70, 89, 107. Justice White appeared most dissatisfied with the ruling, particularly because he felt that the New York legislature jumped through the requisite hoops to enact the statute. *Id.* at 109-111. Justice White's wrath is most directly aimed at Congress for failing to clarify wiretapping and surveillance rules despite substantial indication that it was going to be a matter of great concern between the executive and the judiciary. *Id.* at 112-19.

[56] *Id.* at 55-56.

[57] *Id*. at 119.

[58] *Id*.

[59] Berger v. New York, 388 U.S. at 128.

should be outlawed" and limited the Report by explaining "matters affecting the national security not involving criminal prosecution are outside the Commission's mandate, and nothing in this discussion is intended to affect the existing powers to protect that interest."[60]

Just six months later in 1967, the Supreme Court further expanded the constitutional right to privacy in *Katz v. United States*.[61] In *Katz*, a man inside a public phone booth engaged in illegal wagering over the telephone.[62] Agents of the Federal Bureau of Investigation ("F.B.I.") had placed recording devices just outside of the phone booth that it used to listen to the man's conversations, and introduced the recordings into evidence.[63] The District Court for the Southern District of California convicted defendant on eight counts of transmitting wagering information, and the Ninth Circuit Court of Appeals affirmed the conviction and rejected the argument that the F.B.I. obtained the evidence in violation of the Fourth Amendment.[64] The Supreme Court reversed, holding that Fourth Amendment's privacy protections extended to electronic surveillance and phone conversations specifically.[65] Additionally, through Justice Harlan's concurring opinion, *Katz* established a two-part test for whether an individual has an expectation of privacy that, when violated, can result in the exclusion of evidence. The test finds an expectation of privacy if: (1) the individual had a subjective expectation of privacy, and (2) society recognizes this subjective expectation of privacy as reasonable.[66] The importance of this case is twofold: first, it reinforced the Court's understanding of an implied right to individual privacy in the Constitution, and, secondly, it demonstrated the Court's willingness to engage in a balancing test when comparing this individual right to privacy against the government's interest in surveillance.[67]

---

[60] *Id.* at 129.
[61] 389 U.S. 347.
[62] *Id*. at 348-49.
[63] *Id*.
[64] *Id*. at 348.
[65] *Id*. at 359.
[66] Katz v. United States, 389 U.S. at 360-61 (Harlan, J., concurring); Terry v. Ohio, 392 U.S. 1, 9 (1968) (adopting Justice Harlan's concurring analysis).
[67] Banks & Bowman, *supra* note 29, at 47 (2001). *See also* Christopher Woo & Miranda So,*The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance*, 15 Harv. J. L. & Tech. 521, 523 (2002) (explaining that Justice Harlan's concurring opinion has become the "the governing standard for defining when a Fourth Amendment search occurs and has been used by courts to determine whether a new technology comes within the scope of the Fourth Amendment").

The Court's narrowing of *Katz* is also important. Much as the Court did just six months earlier,[68] the *Katz* decision included two caveats, both pertaining to national security concerns.[69] First, Justice Stewart's majority opinion included a footnote explaining that the question of national security is not an issue presented to the court.[70] Secondly, in a brief concurrence, Justice White reiterated his interpretation that the warrant requirement should not extend to national security matters in which the President and/or the Attorney General have "authorized electronic surveillance as reasonable."[71] Although not explicitly, Justice White appeared to be calling upon Congress to act with regard to the distinction between electronic surveillance for law enforcement purposes and for national security purposes.[72]

C. Congress Responds to the Inadequacies of Katz

1. Enactment of Title III

Congress promptly acquiesced to Justice White's subtle suggestion from *Katz*, and passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[73] widely referred to as Title III.[74] Title III embraced the holdings of *Katz* and *Berger* by codifying the rights to privacy in oral communications[75] and wire communications.[76] Title III requires that if the government wishes to begin oral or wire surveillance, it must obtain a warrant before beginning surveillance.[77] Additionally, Title III establishes a uniform standard under which the government

---

[68] *See Berger*, 388 U.S. at 129 (noting that the holding does not pertain to national security concerns).

[69] *See Katz*, 389 U.S. 347 (1967).

[70] *Id.* at 358 n.23 (1967) (explaining "[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case").

[71] *Id.* at 363-64 (1967) (White, J. concurring).

[72] *Id.* at 363.

[73] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, 211-25 (codified as amended at 18 U.S.C. 2510-2522 (2000)).

[74] Ric Simmons, *From Katz To Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-first Century Technologies*, 53 Hastings L.J. 1303, 1339 (2002).

[75] 18 U.S.C. § 2510(2) (1994); Orin S. Kerr, *Are We Overprotecting Code? Thoughts on First-Generation Internet Law*, 57 Wash & Lee L. Rev. 1287, 1299 (2000). Professor Kerr notes that that the protection of wire communications "did not include the requirement that the communications support a reasonable expectation of privacy" because in 1968 all wire communications were between two humans, and such a requirement would have seemed "superfluous."

[76] 18 U.S.C. § 2510(1) (1994).

[77] 18 U.S.C. § 2518 (1968).

may pursue a warrant.[78] Specifically, to obtain a warrant, the government must demonstrate that it (1) has probable cause against the target of the surveillance;[79] (2) has a special need to conduct electronic surveillance;[80] and (3) will minimize the interception of innocent communications.[81] Furthermore, a target of electronic surveillance under Title III has the right to learn about the surveillance and challenge the probable cause against him, and may demand the exclusion of any evidence obtained against him if the government has violated Title III in obtaining the evidence.[82]

Title III extends to third party intrusion on individual privacy through a broad application of the exclusionary rule as the remedy available. The evidentiary prohibition portion of Title III stipulates the following[83]:

> Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

In applying an exclusionary remedy to a victim of illegal interception, Congress maintained Title III's connection to the Fourth Amendment common law remedy.[84]

For a short time after its enactment, individual privacy with respect to electronic communications fell largely under the purview of Title III.[85] Although not explicit in the statute's language, Title III embraced Justice Harlan's "reasonable expectation of privacy" test from *Katz*.[86] While Title III extended to the suppression of oral or wire communications that were *intercepted* by third

---

[78] *Id.*; Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. Chi. L. Rev. 287, 290 (2008).

[79] 18 U.S.C. § 2518(3) (2000).

[80] 18 U.S.C. § 2518(3)(c) (2000).

[81] 18 U.S.C. § 2518(5) (2000).

[82] Nathan C. Henderson, *The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications*, 52 Duke L. J. 179, 183 (2002).

[83] 18 U.S.C. § 2515.

[84] *Id.* at 182-83.

[85] Kerr, *surpa* note 75, at 1299; Simmons, *supra* note 74, at 1339-41.

[86] Simmons, *supra* note 74, at 1340 (explaining § 2510 of Title III and connecting it to Justice Harlan's concurring opinion in *Katz*).

parties, Title III did not account for the fact that individuals voluntarily share information with third party telecommunications companies during the course of normal interaction.[87] It soon became clear that the Fourth Amendment did not protect this information either, when the Supreme Court narrowed the scope of the Fourth Amendment's privacy protections with regard to this voluntarily shared information in two landscape-altering cases.

2. Miller, Smith, and the Court's Narrowing of Fourth Amendment Privacy Protections

In 1976 and 1979, the Supreme Court decided *United States v. Miller*[88] and *Smith v. Maryland*,[89] commonly referred to as the "business record" cases.[90] The holdings of *Miller* and *Smith* significantly marginalized *Katz*.[91] Specifically, these cases jointly established that the temporary-yet-voluntary possession of an individual's information by a third party precluded a legitimate expectation of privacy in that information, thus precluding application of the exclusionary rule to that information.[92]

In *Miller*, agents from the Bureau of Alcohol, Tobacco, and Firearms subpoenaed defendant's bank account to demonstrate that he was engaged in several illegal acts, including prohibition-related offenses and tax fraud.[93] The government used the defendant's bank account information to convince the district court to convict him after denying his motion to suppress the bank account information from evidence on Fourth Amendment grounds.[94] The Court of Appeals for the Fifth Circuit reversed the conviction, citing *Boyd v. United States*[95] and determining that the government's subpoena of the defendant's bank account information was a Fourth Amendment violation.[96] The Supreme Court reversed, holding that the defendant did not have a reasonable expectation of privacy with

---

[87] Patricia L. Bellia, *Surveillance Law through Cyberlaw's Lens*, 72 Geo. Wash. L. Rev. 1375, 1396 (2004).

[88] U.S. v. Miller, 425 U.S. 435 (1976).

[89] Smith v. Maryland, 442 U.S. 735 (1979).

[90] Marc J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not a Level Playing Field*, 97 J. Crim. L. & Criminology 569, 574 (2007).

[91] *Id.*

[92] Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, *supra* note 21, at 1209-10.

[93] *Miller*, 425 U.S. at 437.

[94] *Id.* at 438-39.

[95] 116 U.S. 616 (1886).

[96] *Miller*, 425 U.S. at 439.

regard to his bank records because he voluntarily disclosed the records to the bank.[97] The Court stressed that the Fourth Amendment "does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."[98]

Just three years later, the Court fortified its holding in *Miller* by holding that an individual does not have a legitimate expectation of privacy with regard to the phone numbers he dials from his house.[99] In *Smith v. Maryland*, the police requested and the phone company agreed to install a pen register[100] at the telephone company's offices that recorded the numbers the defendant dialed from home.[101] The *Smith* Court applied both prongs of Justice Harlan's *Katz* test to determine whether the Fourth Amendment applied to the phone numbers that the defendant dialed. First, the Court concluded that a telephone user should not have a subjective expectation of privacy in telephone numbers dialed because "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company."[102] Secondly, the Court reasoned that even if the defendant had a subjective expectation of privacy, such expectation is not one that the society recognizes as reasonable.[103] The Court held that the telephone user "assumed the risk" that the government would obtain these telephone numbers, and reiterated its stance in *Miller* that a person does not hold a legitimate expectation of privacy in information he turns over to a third party.[104] As it turns out, *Smith* was just the beginning of widespread confusion when applying Fourth Amendment principles to developing technologies.

D. The Clean Hands Exception: An Avenue for Introducing Illegally Obtained Evidence into the Courtroom

Early legislative efforts in response to the business records cases granted a broad range of individual privacy protections.[105] However, one important instance of discord centered around whether the government should be allowed to introduce

---

[97] *Id.* at 440.

[98] U.S. v. Miller, 425 U.S. 435, 443 (1976).

[99] *Smith*, 442 U.S. at 735.

[100] At the time of the case, a pen register was understood to mean "a device that records the numbers dialed on a telephone by monitoring electrical impulses caused when the dial is released." Bellia, *supra* note 87, at 1427-28.

[101] *Smith*, 442 U.S. at 737.

[102] *Id.* at 742.

[103] *Id.* at 743.

[104] *Id.* at 744.

[105] *See infra* Part I.C

into evidence information obtained illegally by a third party but which the government did not play a part in obtaining.[106] Commonly referred to as the "clean hands" exception, the question is one that continues to split federal circuits.[107] The most modern seminal "clean hands" case is *United States v. Murdock*,[108] in which the Sixth Circuit held that the government was allowed to introduce evidence of a man's criminal conduct that was recorded illegally by the man's wife.[109]

1. Factual and Procedural Background

In *Murdock*, a wife became suspicious of her husband's dealings, both personally and professionally.[110] As a result, she began recording conversations from the family business telephone line on an extension of the business' telephone line connected to the family's home.[111] After seeing a story in the local paper about the negotiations between the school board and a local dairy, the wife became convinced that her husband, who was president of the school board, was acting improperly.[112] She went back and listened to her recordings, and found evidence of her husband accepting a bribe from the local dairy.[113] The wife forwarded the information to a competing dairy, who in turn forwarded the information to the local newspaper.[114] An investigation ensued, and the government eventually used this information to charge the husband for income tax evasion because he failed to report the bribe as income.[115] The husband then moved to suppress the evidence

[106] Francis M. Hamilton, III, *Should "Clean Hands" Protect the Government Against § 2515 Suppression Under Title III of the Omnibus Crime Control and Safe Streets Act of 1968?*, 53 Wash & Lee L. Rev. 1473, 1480 (1996).

[107] Olsen, *supra* note 13, at *749.*

[108] 63 F.3d 1391 (6th Cir. 1995).

[109] *Id.*

[110] *Id.* at 1392-93

[111] *Id.*

[112] *Id.*

[113] *Id.*

[114] *Id.*

[115] *Id.* at 1393-94. The "business extension exemption" is a limit on the applicability of Title III, and exempts the monitoring of communications carried out in the normal course of business. The court of appeals determined that despite the fact that the family's business had a phone line in the house, the nature of the monitoring was not consistent with normal business practices. For more information regarding the business extension exemption, *see* Thomas R. Greenberg, *E-mail and Voice Mail: Employee Privacy And The Federal Wiretap Statute*, 44 Am. U. L. Rev. 219, 239 (1994).

under Section 2515 of Title III,[116] which provides for the exclusion of evidence obtained through illegal surveillance.[117]

The district court denied the defendant's motions to suppress on two grounds. First, the court held that the statutory prohibitions of Title III did not apply in this case because of the business line extension in the family's home.[118] The Court explained that Sections 2510(4) and 2510 (5) provide an exception to the statutory prohibition of electronic surveillance that occur in the place of business and during the ordinary course of business.[119] The Sixth Circuit reversed this holding, yet conceded that the wife's monitoring of her husband was in fact a violation of Section 2515 of Title III.[120] Second, the district court held alternatively that the exclusionary remedy for a Title III violation did not apply to the government "where it played no part in the interception of the conversation."[121] The Sixth Circuit agreed with this conclusion, and affirmed the lower court's decision that the government was entitled to a "clean hands" exception to the Title III exclusionary rule.[122]

2. The Court's Rationale

The Sixth Circuit's holding in *Murdock* rested on the fact that the government did not play a part in the illegal electronic recording activity.[123] This led the court to reason that the public policy interest in allowing the evidence into court outweighed an interpretation of the applicable law in favor of the defendant.[124] In reaching this conclusion, the Sixth Circuit analyzed competing theories of Title III and Fourth Amendment jurisprudence.

First, the court reanalyzed the legislative history of Section 2515, and determined that the statute only aimed to protect victims of unlawful interception from the perpetrator's use of the information against the victim.[125] In so holding, the *Murdock* court distanced itself from *United States v. Vest*,[126] the initial case to

---

[116] *Murdock*, 63 F.3d at 1393.
[117] 18 U.S.C. § 2515 (1968).
[118] *Murdock*, 63 F.3d at 1393.
[119] *Id.* (citing Williams v. Poulos, 11 F.3d 271, 279 (1st Cir.1993)).
[120] *Id.*
[121] *Id.*
[122] *Id.* at 1404.
[123] *Id.* at 1402-04. The applicable law in the matter was 18 U.S.C. § 2515.
[124] *Murdock*, 63 F.3d at 1402-04. The applicable law in the matter was 18 U.S.C. § 2515.
[125] *Id.* at 1403.
[126] United States v. Vest, 813 F.2d 477 (1st Cir. 1987).

invoke the clean hands exception.[127] In *Vest*, the government prosecuted a man for acting as a conduit in the bribery of a Massachusetts police officer.[128] A criminal defendant made an illegal recording of his payment to a Boston police officer as part of a bribe to ensure a lenient sentence.[129] When the police officer claimed that he had not received the payment, the defendant turned over the recording to the authorities.[130] The government attempted to introduce the recording as evidence against the police officer.[131] However, the First Circuit rejected the government's argument.[132] The court relied on the 1972 Supreme Court case *Gelbard v. United States*[133] to demonstrate Title III's broad implications regarding fundamental privacy rights, and reiterated the finding that "the protection of privacy was an overriding congressional concern . . . and that secton 2515′s importance as a protection for the victim of an unlawful invasion of privacy could not be more clear."[134] The *Gelbard* court relied on a 1968 Senate Report supplementing the passage of Title III, which read in pertinent part[135]:

> Virtually all concede that the use of wiretapping or electronic surveillance techniques by private unauthorized hands has little justification where communications are intercepted without the consent of one of the participants. No one quarrels with the proposition that the unauthorized use of these techniques by law enforcement agents should be prohibited. . . . Only by striking at all aspects of the problem can privacy be adequately protected. The prohibition, too, must be enforced with all appropriate sanctions. Criminal penalties have their part to play. But other remedies must be afforded the victim of an unlawful invasion of privacy. Provision must be made for civil recourse for damages. The perpetrator must be denied the fruits of his unlawful actions in civil and criminal proceedings. Each of these objectives is sought by the proposed legislation.

---

[127] *Id.*
[128] *Id.* at 481.
[129] *Id.* at 479.
[130] *Id.*
[131] *Id.*
[132] *Id. at 481.*
[133] 408 U.S. 41 (1972).
[134] *Vest*, 813 F.2d at 481 (internal quotations omitted) (citing Gelbard v. United States, 408 U.S. 41, 47-52 (1972)).
[135] S. Rep. No. 1097, 90th Cong., 2d Sess., 66 (1968) (quoted in Gelbard v. United States, 408 U.S. 41, 47-52 (1972)).

The *Vest* court also based its conclusion on the grounds that the government should not receive a clean hands exception when prosecuting a case in which the government would not have been able to receive a wiretap warrant.[136] A Title III warrant for electronic surveillance is only available when an appropriate magistrate determines that such surveillance will lead to evidence of an enumerated crime.[137] Perjury is not one of the enumerated crimes, and the police therefore would not have been able to obtain a wiretap to demonstrate the police officer's perjury.[138]

The *Vest* court's rationale for rejecting a clean hands exception has most been embraced more recently by the Third Circuit in *In re Grand Jury*.[139] The Third Circuit, in relying on *Vest* and explicitly rejecting *Murdock*, concluded that refusing to suppress the evidence might have been plausible had the court interpreted a conflict between the plain statutory reading of Section 2515 and available legislative history.[140] However, the court found no conflict, and emphasized a lack of legislative history suggesting a suspension of the suppression remedy.[141]

The *Murdock* court disagreed with the *Vest* court's analysis of the legislative history, and instead interpreted the legislative statements to read that Section 2515 did nothing to alter the traditional Fourth Amendment analysis that accompanies a search.[142] Thus, the court reasoned that like traditional Fourth Amendment procedure that does not require suppression of evidence that police obtain [in good faith / due to luck / etc.], the Fourth Amendment and Title III in no way require courts to suppress oral and wire surveillance evidence when the police obtain that evidence merely through a lucky break.[143] In support, the court cited the Sixth Circuit case *United States v. Underhill*[144] in demonstrating the principle that evidence suppression under Section 2515 does not occur in all circumstances.[145] Nonetheless, the *Murdock* court held that Section 2515 did not intend to create a loophole through which a defendant could escape

---

[136] *Vest*, 813 F.2d at 481.
[137] 18 U.S.C. 2516(1)(b) (1986).
[138] *Id.*
[139] In re Grand Jury, 111 F.3d 1066, 1068 (3rd Cir. 1997).
[140] *Id.* at 1077.
[141] *Id.*
[142] *Murdock*, 63 F.3d at 1402-03.
[143] *Id.* at 1403.
[144] 813 F.2d 105 (6th Cir. 1987).
[145] *Murdock*, 63 F.3d at 1402 (citing United States v. Underhill, 813 F.2d 105, 111-112 (6th Cir. 1987)).

liability.[146] The *Murdock* court also considered it vital that a suspension of the suppression remedy in such circumstances would in no way adversely encourage police officers from violating Title III.[147]

The *Murdock* court also relied heavily on *United States v. Baranek*,[148] which held that the government could introduce evidence obtained when a defendant failed to properly hang up a phone after a legally wiretapped conversation.[149] The court in *Baranek* explained that the government caught a "lucky break," and that allowing the introduction of this evidence into court would be consistent with 18 U.S.C. Section 2515.[150] The *Murdock* court came to a similar conclusion, finding the wife's illegal recording and subsequent disclosure of the telephone conversation to the police analogous to the lucky break in *Baranek*.[151] The court found especially compelling the argument that allowing the evidence into trial "would not create the problem of government agents encouraging violations of Title III."[152]

3. The Present Status of the Clean Hands Exception

The Sixth Circuit stands alone in its analysis of the clean hands exception, however, as several other circuits have reasoned that a plain language reading of the statutory exclusionary rule leaves no room for the creation of a clean hands exception.[153] These courts hold that the deterrent effect of the exclusionary rule maintains its applicability even when the government has clean hands. These courts emphasize that the Fourth Amendment exclusionary rule, on which the Title III rule is based, is a judicial construct whereas the rule set forth in Title III is a congressionally-created mechanism.[154] The fact that the rule has a statutory foundation provides less leeway for the courts in determining when and how to

---

[146] *Id.* at 1403.
[147] *Id.* at 1402.
[148] 903 F.2d 1068 (6th Cir. 1990).
[149] *Id.*
[150] *Id.* at 1072.
[151] *Murdock*, 63 F.3d at 1402-03.
[152] *Id.* at 1402.
[153] *See* United States v. Crabtree, 565 F.3d 887, 889 (4th Cir. 2009); Chandler v. U.S. Army,125 F.3d 1296, 1302 (9th Cir. 1997); In re Grand Jury, 111 F.3d 1066, 1079 (3d Cir. 1997); United States v. Vest, 813 F.2d 477, 481 (1st Cir. 1987) (all holding that a plain reading of § 2515 does not allow for a clean hands exception to be granted to the government in an illegal surveillance case).
[154] *See, e.g.*, United States v. Vest, 813 F.2d 477, 481 (1st Cir. 1987).

implement the rule.[155] In 2009, the Fourth Circuit became the most recent Court of Appeals to hear the matter, and sided with the plurality of federal courts of appeal.[156] The court shared much of the reasoning of prior courts, and added that Congress' silence regarding the ambiguous statute reinforces the plurality's interpretation, as Congress has had ample time to clarify the statute's meaning.

Nestled within the debate of whether a clean hands exception exists under Title III is whether a plain language reading of the Title III leads one to a natural conclusion that Title III contains a clean hands exception. The *Murdock* court certainly believed the plain language reading was ambiguous, and looked to legislative intent in deciding the case, declaring "[t]here is nothing in the legislative history which requires that the government be precluded from using evidence that literally falls into its hands."[157] The First Circuit, on the other hand, saw no ambiguity in the statute as written, and refused to extend a "clean hands" exception, explaining "the government's use of unlawfully intercepted communications where the government was not the procurer would eviscerate the statutory protection of privacy from intrusion by illegal private interception."[158] Congress has declined any opportunity to clarify its meaning, instead leaving the federal courts to battle out the existence and utility of a plain meaning reading of the statute.

The clean hands exception functions as the "alter ego" of the good faith exception highlighted by the Court in *Leon*.[159] The Court has applied the good faith exception narrowly, limiting it only to police officers in the field and not applying it to situations in which a Title III exclusionary rule question arises with respect to the third party surveillance.[160] In essence, a good faith argument against suppression of evidence may be replaced by one of clean hands in situations of third party monitoring.[161] One key distinction, however, is that in many situations of good faith, the officers in question may not be acting illegally, whereas an

---

[155] Matthew A. Josephson, *To Exclude Or Not To Exclude: The Future of the Exclusionary Rule After Herring v. United States*, 43 Creighton L. Rev. 175, 180 (2009).

[156] *Crabtree*, 565 F.3d at 890.

[157] *Murdock*, 63 F.3d at 1403.

[158] *Vest*, 813 F.2d at 481 (internal quotations omitted). For an article discussing the accuracy of the First Circuit's logic, *see* Hamilton, *supra* note 106, at 1506.

[159] *See* Precision Instrument Mfg. Co. v. Auto. Maint. Mach. Co., 324 U.S. 806, 814-15 (1945)(holding that "clean hands" is essentially a vehicle for the implementation of the "good faith" doctrine); *see also* Castle v. Cohen, 840 F.2d 173, 178 (3d Cir. 1988) (holding that "clean hands" is simply another expression of "good faith"); Olsen, *supra* note 13, at *722.*

[160] Olsen, *supra* note 13, at 722.

[161] *Id.*

individual monitoring the communications of another is engaging in a violation of Title III.[162]

E. The Stored Communications Act

The combination of the business record cases and the rapid development of new technologies forced Congress to again address the nexus between Fourth Amendment individual privacy concerns and communications.[163] Specifically, due to the business records cases, any info transmitted voluntarily to a third party has no legitimate expectation of privacy, and thus is unprotected by the Fourth Amendment. Since more and more people are using email, which necessarily passes through a third party ISP, this suggests that a key way that people communicate is unprotected by the Fourth Amendment. In 1986, understandably concerned about the privacy of electronic communications, Congress passed the ECPA.[164] [165] Congress' purpose behind the ECPA was to extend Fourth Amendment privacy principles to electronic communications and to regulate "the relationship between government investigators and electronic service providers in possession of users' private information."[166]

The ECPA contains three primary sections: The Wiretap Act, the Pen Register Act ("PRA"), and the SCA.[167] The SCA alone regulates past and stored information,[168] whereas the PRA and the Wiretap Act both govern "communications in transit," limiting application of these statutes to transmission of information occurring in the moment.[169] These statutes can also be distinguished on practical grounds. Whereas telecommunications companies providing services governed by the PRA and the Wiretap Act only have fleeting access to the content of their customers' communication, ISPs (as well as mobile phone companies storing either voicemail or text messages) maintain access to this information for as long as a customer chooses to leave the information on the server without

---

[162] 18 U.S.C. § 2511(1)(a). The court has noted some exceptions, most notably the business extension exemption. *See supra* note 94.

[163] Bellia, *supra* note 87, at 1396; Michael S. Leib, *E-Mail and the Wiretap Laws: Why Congress Should Add Electronic Communication to Title III's Statutory Exclusionary Rule and Expressly Reject a "Good Faith" Exception*, 34 Harv. J. on Legis. 393, 396 (1997).

[164] Pub. L. No. 99-508, § 101(c), 100 Stat. 1848, 1851-52 (1986) (changes various portions of Title III, 18 U.S.C.).

[165] Leib, *supra* note 163, at 402-04.

[166] Kerr, *supra* note 21, at *1212.*

[167] Rosenbloom, *supra* note 7, at 538 n.151.

[168] 18 U.S.C. §§ 2701-2712 (1986).

[169] 18 U.S.C. §§ 2511-2522 (1986)

deleting it.[170] A 1985 Congressional study into the privacy implications for technologies to be governed by the ECPA concluded the following with respect to ISP practices:

> All electronic mail companies retain a copy of the message both for billing purposes and as a convenience in case the customer loses the message. Based on the reasoning in *United States v. Miller*, 425 U.S. 435 (1976), where the Court ruled that records of financial transactions, including copies of personal checks, were the property of the bank and that an individual had no legal rights with respect to such records, it is possible that an individual would not have a legal basis from which to challenge an electronic mail company's disclosure of the contents of messages or records of messages sent.[171]

Stored communications can include both content and non-content information,[172] but the protections enacted in the SCA seek to fortify an individual's privacy with respect to the content of his electronic communication.[173]

---

[170] Federal Government Office of Technology Assessment: Electronic Surveillance and Civil Liberties 45 (1985); *See also,* Leib, *supra* note 163, at 404-05 (explaining ISPs practice of retaining copies of customers' emails for administrative purposes).

[171] Federal Government Office of Technology Assessment: Electronic Surveillance and Civil Liberties 45 (1985).

[172] The content/non-content distinction is often referred to as the "Content/Envelope Distinction." The analogy is clear: there is a difference between the actual content and information transmitted between two parties, and the information required to direct a third party transmitter (such as a telephone company or ISP) to the correct recipient. For more information regarding the distinction, *see,* Achal Oza, *Amend the ECPA: Fourth Amendment Protection Erodes as E-mails Get Dusty*, 88 B.U. L. Rev. 1043, 1049 (2008).

[173] While not completely resolved, court and commentators largely agree that non-content information is not protected by the Fourth Amendment. *See, e.g.*, Warshak v. United States, 532 F.3d 521, 525-27 (6th Cir. 2008) (holding that an individual has a reasonable expectation of privacy to the content of his email, but not to the transactional information). *See also* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007) (holding that ISP transactional information was "constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*"). Congress eventually recognized that transactional envelop information pertaining to e-mail revealed considerably more about a person than the numbers he dials on a telephone. As a result Congress stopped allowing law enforcement to obtain this information through subpoena in 2000 through the Communications Assistance for Law Enforcement Act (CALEA), and instead limited access to such information to a court order. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994). For more information about CALEA, see Henderson, *supra* note 82, at 183.

1. The Statute's Protection Against Compulsory Disclosure

On its face, the SCA extends a broad range of protection to customers and consumers of electronic communications service providers ("Providers"), such as ISPs. Section 2701 provides both criminal and civil penalties for either accessing without authorization "a facility through which an electronic communication service is provided" or exceeding one's authorization in accessing such facility.[174] However, Section 2701(c) nullifies these punishments in instances in which either an electronic communication service provider or the user of that service authorizes the access.[175] Some commentators have pointed out another limitation to the statute. The provision applies only to electronic communications services ("ECS")[176] and, through omission, does not apply to facilities in which a remote computing service ("RCS")[177] is provided.[178] This distinction is drawn out in later sections of the SCA, but an understanding of the differences between the two services is necessary to comprehend the SCA.

Professor Orin Kerr best explains the distinction between ECS and RCS by breaking down the life of an e-mail into its two core parts: (1) transmission of communication; and (2) storage of that communication in its electronic form.[179] When an e-mail is sent to another person through a Provider, the Provider is acting as an ECS with respect to that message—it is providing the user with the ability to transmit the communication, as well as temporary storage.[180] However, if that e-mail stays on the Provider's server beyond a temporary status, statutorily defined as 180 days,[181] the very same Provider becomes an RCS in that it is providing computer storage or processing to the public.[182] This is true regardless of whether the recipient has read the message. The distinction is further complicated by the

[174] 18 U.S.C. § 2701 (a)-(b) (1986).

[175] 18 U.S.C. § 2701 (c) (1986).

[176] The statute defines electronic communications services as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510 (15) (1986).

[177] The statute defines remote computing service as "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2) (1986).

[178] Bellia, *supra* note 87, at 1415.

[179] Kerr, *A User's Guide to the Stored Communications Act*, *supra* note 21, at 1216-18.

[180] *Id.* at 1215-16.

[181] The 180 day threshold is provided by the compelled disclosure provision of the SCA, found at 18 U.S.C. 2703 (1986). *See infra* Part 2.

[182] Kerr, *A User's Guide to the Stored Communications Act*, *supra* note 21, at 1215-16.

fact that most modern ISPs provide both ECS and RCS through their normal procedures.[183]

In certain circumstances, the SCA requires that a Provider disclose information to the government when the government follows certain specified procedures to request it. Compulsory disclosure under the SCA is governed by Section 2703 and trumps the disclosure limitations set out in Section 2701(c), meaning that neither the government nor the Provider suffers any criminal or civil penalties for disclosure.[184] Section 2703 considers three types of electronic communications: (1) those held by an ECS for 180 days or less; (2) those held by an ECS for more than 180 days; and (3) those held by an RCS.[185] The 180 day cut-off period becomes extremely important when the government is seeking a compulsory disclosure. Communications in the first group may only be compelled if the government obtains a warrant through normal Fourth Amendment probable cause standards.[186] But, communications in either the second or third group allow the police to compel the information by either obtaining a warrant, or obtaining a grand jury or administrative subpoena.[187] The government may also obtain the information through a court order provided that the government informs the customer of the subpoena or court order after the fact.[188] This tangled compulsory disclosure languages creates a difficult situation for the government seeking evidence in a criminal or national security investigation.[189]

2. The Statute's Allowance of Voluntary Disclosure

One pivotal distinction between the SCA and its counterparts enacted under the ECPA is the existence of a voluntary disclosure option.[190] While all three parts of the ECPA contain language governing compulsory disclosure by a Provider, the

---

[183] LaFave, Criminal Procedure, *supra* note 45, at § 4.8(d); U.S. Internet Service Provider Association, *Electronic Evidence Compliance–A Guide for Internet Service Providers*, 18 Berkeley Tech. L.J. 945, 949 (2003).

[184] Bellia, *supra* note 87, at 1416.

[185] 18 U.S.C. § 2703 (1986).

[186] 18 U.S.C. § 2703(a) (1986).

[187] *Id.*

[188] 18 U.S.C. § 2703(b)-(c) (1986).

[189] The Department of Justice Computer Crimes and Intellectual Property Section officially interprets Section 2703(d) to mean that the government can access, through subpoena, any copies of electronic communication at any time after the recipient of the communication has accessed it. For more information, *see*, Office of Legal Education, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (Richard Downing et al. eds., 3rd ed. 2009), *available at*http://www.cybercrime.gov/ssmanual/ (last visited April 19, 2010).

[190] Rosenbloom, *supra* note 7, at 538-39.

SCA alone contains a provision that allows Providers to independently and voluntarily supply certain information to the government in specific circumstances.[191] Sections 2702(b) and 2702(c) govern the voluntary disclosure of customer communicative information by Providers.[192] The disclosure of customer non-content, customer records falls under 2702(c), and overrides the limits set forth in Section2702(a).[193]

Section 2702(b) provides the voluntary disclosure rules pertaining to content information.[194] In the case of stored communications, the content information consists of the actual communication within the body of an email.[195] The envelope information consists of the sending and receiving email addresses, IP addresses, and email subject lines.[196] For the purposes of assessing the connection between the clean hands exception and the SCA, the provisions controlling content information in Section 2702(b) are much important. Section 2702(b) reads as follows:

> (b) Exceptions for disclosure of communications. A provider described in subsection (a) may divulge the contents of a communication–
>
> (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
>
> (2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title [18 U.S.C. § 2517, 2511(2)(a), or 2703];
>
> (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;
>
> (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

---

[191] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 284-85; Rosenbloom, *supra* note 7, at 538.

[192] 18 U.S.C. §§ 2702(b)-(c) (1986).

[193] 18 U.S.C. § 2702(a) (1986).

[194] 18 U.S.C. §§ 2702(b)-(c) (1986)

[195] Rosenbloom, *supra* note 7, at 543-44.

[196] *Id.*

> (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
>
> (6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A [18 U.S.C. § 2258A];
>
> (7) to a law enforcement agency– (A) if the contents–(i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime; or
>
> (8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

The first seven enumerated circumstances all pertain to either an individual's right to control his own information, or a particular government purpose. The eighth provision is unlike the previous seven in that it (1) allows for a great deal of discretion, and (2) allows Providers to make the determination regarding both the severity of the emergency and the exigency with which the government will require the information.[197]

Significantly, Section 2702(b)(8) did not always exist, so Providers were not always allowed to disclose purely because there was an "emergency" situation.[198] Prior to its enactment, the SCA allowed for voluntary disclosure only when two stipulations were satisfied: First, the information had to be *inadvertently* obtained by the service provider.[199] Second, the information had to relate to a crime.[200] In response to critical national security concerns in the wake of 9/11, and to give law enforcement personnel an enhanced ability to detect and prevent crimes, Congress significantly amended Section 2702(b)(8), otherwise known as the "emergency disclosure provision."[201] The following subpart discusses the evolution of this provision.

---

[197] Gorelick, *supra* note 1, at *361 n.53.*
[198] 18 U.S.C. § 2702(b)(6)(A) (2000).
[199] *Id.*
[200] 18 U.S.C. § 2702(b)(6)(A) (2000).
[201] Rosenbloom, *supra* note 7, at 559-60.

3. Significant Amendments to 2702(b)(8) in the Wake of 9/11

Over the course of fourteen months immediately after 9/11, Congress made four critical changes to the voluntary disclosure provisions of Section 2702(b) which greatly increased the scope of provision and ISPs' discretion.[202] Pursuant to Section 212 of the USA PATRIOT Act, on October 26, 2001 the government first expanded the scope of the voluntary disclosure by allowing an ISP to divulge content information to law enforcement if it believed "an emergency involving immediate danger of death or serious physical injury to any person" was imminent.[203]

Just one year after the PATRIOT Act modifications, in November of 2002, Congress passed the Homeland Security Act which again expanded the scope of voluntary emergency disclosure.[204] This modification provided three significant changes to the statute. First, Congress allowed for disclosure in the instance of "serious physical injury," thereby eliminating the previous "danger of death" requirement.[205] Secondly, the Homeland Security Act removed the "reasonable belief" requirement, leaving only a "good faith belief" standard.[206] Thirdly, Congress included a requirement that the communication disclosed through Section 2702(b)(8) "relate to the emergency" but also expanded ISPs' options by allowing them to disclose to any federal, state, or local government entity instead of strictly a law enforcement official.[207] Aside from a small alteration in the USA PATRIOT Improvement and Reauthorization Act of 2005, in which Congress clarified that content and noncontent information should be treated identically, Section 2702(b)(8) remains unchanged and, perhaps surprisingly, widely unlitigated.[208]

---

[202] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 284-85; *Id.* at 559-60.

[203] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 284-85.

[204] Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135, 2157.

[205] Rosenbloom, *supra* note 7, at 559-60.

[206] *Id.*

[207] *Id.*

[208] Rosenbloom also notes a fourth change in the 2006 USA PATRIOT Act Improvement and Reauthorization Act in which Congress officially removed any barriers separating the rules for content disclosure and noncontent disclosure by inserting the broadly defined phrase "communications relating to the emergency". *Id.*; USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177, 120 Stat. 192, 202-03 (2006).

The amendments to the voluntary disclosure provisions were immediately controversial. The amendments met faced criticism during Congressional debates.[209] The debate featured those who insisted that the amendments were necessary to enable law enforcement and homeland security professionals access to vital information in a timely manner. On the other hand, many privacy advocates argued that the amendments overstepped Fourth Amendment boundaries. Alan Davidson of the Center for Democracy and Technology explained "the emergency disclosure provision of section 102 as drafted currently is overly broad, and we fear would eviscerate some important privacy protections that exist in the law right now…our fear is that these voluntary disclosures are turning into a major loophole in current law, because small providers are not in a position to evaluate these requests when they come, and of course, just turn around and provide this information."[210] Congress also included a check against voluntary disclosure abuses via Section 2702 by requiring the Attorney General to submit an annual report containing the number of voluntary disclosures received by the Department of Justice to the Committee on the Judiciary of the House of Representatives and Committee on the Judiciary of the Senate.[211] This report must also contain the basis for disclosure for all instances in which the Department of Justice closed an investigation without filing charges against the ISP user in question.[212]

It is noteworthy that Congress continues to introduce legislation in efforts to limit the broad scope of the emergency exception.[213] In late 2009, Senators Feingold and Leahy, joined by Representatives Conyers and Nadler in the House, proposed legislation to re-amend the language of the emergency disclosure provision.[214] The legislation proposed to insert an immediacy requirement for the disclosure.[215] This would limit the number of circumstances in which the Providers

---

[209] *See, e.g.*, Cyber Security Enhancement Act of 2001 Hearing Before the H. Subcomm. on Crime, 107th Cong. 58 (2005), available at http://commdocs.house.gov/committees/judiciary/hju77697.000/hju77697_0f.htm (last visited April 19, 2010).

[210] *Id.*

[211] 18 U.S.C. 2702(d) (2006).

[212] *Id.*

[213] S. 1686, 111th Cong. § 105 (1st Sess. 2009); H.R. 1800, §7. S. 1686, §105 (1st Sess. 2009).

[214] *Id.*

[215] *Id.*

could disclose information, and provide an added level of privacy protection for customers.[216]

4. Remedies Under the SCA

The SCA provides for a different set of remedies against a Provider than it does for an action against an individual in violation of the statute. Section 2701(b) provides for both fines and jail time for violations of the SCA by someone other than a Provider, a user with respect to the communication in question, or the government.[217] Violations made for the purpose of commercial advantage, malicious destruction or damage, for private commercial gain, or in furtherance of an act against the Constitution may receive a fine and/or jail time up to five years for a first offense and 10 years for any subsequent offenses.[218] Violations made in other circumstances may be punished by up to one year imprisonment and a fine.[219]

The only remedy available against a Provider through the SCA is a civil action.[220] The exclusion of evidence is not an available remedy.[221] Moreover, Congress set the bar high, requiring the plaintiff to show the Provider acted "with a knowing or intentional state of mind."[222] However, courts have been generous in awarding damages in successful suits, and may not necessarily require the plaintiff to show actual damages.[223]

5. SCA Voluntary Disclosure Litigation in the Wake of September 11, 2001

Litigation over Section 2702(b) remains scant. The leading case on this provision is *Freedman v. Am. Online, Inc.*,[224] which was decided on Section 2703 grounds after the court explicitly rejected the government's voluntary disclosure

---

[216] Charles Doyle, Congressional Research Service, *National Security Letters: Proposed Amendments in the 111th Congress*, at 20, (Oct. 2009), *available at*http://www.fas.org/sgp/crs/intel/R40887.pdf.

[217] 18 U.S.C. 2701(b) (1986).

[218] *Id.*

[219] *Id.*

[220] 18 U.S.C. 2707 (1986).

[221] United States v. Mercado-Nava, 486 F. Supp. 2d 1271, 1279 (D. Kan. 2007) (explaining that "exclusion of the evidence is not an available remedy for a Title II violation of the ECPA, *see* 18 U.S.C. §§ 2515, 2708. The remedy for such a violation, set forth in 18 U.S.C. § 2707, lies in a civil action against the person or entity who violated the statute").

[222] 18 U.S.C. 2707 (1986).

[223] *See, e.g.*, Konop v. Hawaiian Airlines, Inc. (In re Hawaiian Airlines, Inc.), 355 B.R. 225, 230 (D. Haw. 2006).

[224] 303 F. Supp. 2d 121 (D. Conn. 2004).

argument under Section 2702(b)(8).[225] In *Freedman*, two police officers in Connecticut faxed an unsigned warrant to America Online ("AOL"), an ISP. Believing the warrant to be effectuated properly, AOL complied with the warrant's request and disclosed to the police officers the plaintiff's "name, address, phone numbers, account status, membership information, software information, billing and account information, and his other AOL screen names."[226] The police officers contended that they did not actually require AOL to disclose the information, but rather merely requested it, and that AOL subsequently provided the information in something akin to a voluntary disclosure under Section 2702(b)(8).[227] The court rejected the officer's argument, holding that the officers failed to follow the stipulations set forth in 18 U.S.C. Section 2703(c), and noted that the SCA existed to balance the desire to protect personal privacy with legitimate law enforcement needs.[228]

The *Freedman* court explicitly and purposefully distanced its opinion from how it might rule in an emergency circumstance. The court explained that it "decline[d] to speculate whether it would ever be appropriate, under exigent circumstances when it would not be feasible to get a signed warrant or comply with other legal process, for the government to notify the ISP of an emergency and receive subscriber information without conforming with the ECPA."[229] AOL explained that they believed the warrant was issued correctly, and did not intend to voluntarily disclose any information to the police officers.[230] The net result is a single instance in which the court refused to find a legitimate voluntary disclosure because there was no evidence of volition by the service provider. However, this holding contains a significant caveat that the court might find otherwise if the circumstances were either (1) more similar to an emergency from the law enforcement's perspective; or (2) more founded upon a subjective good faith voluntary disclosure by the ISP.

Freedman differs from *Jayne v. Sprint PCS*,[231] a 2009 case in which the Court for the Eastern District of California determined that the telecommunication provider acted correctly in providing authorities with an individual's cell phone

[225] *Id.* at 124.
[226] *Id.* at 123.
[227] *Id.* at 126-27.
[228] *Id.* at 127.
[229] *Id.* at 128.
[230] AOL successfully dismissed all claims against it relating to this matter on a forum selection clause in the contract, and therefore did not have to litigate the matter. *Freedman*, 303 F. Supp. 2d at 123.
[231] 2009 WL 426117 (E.D. Cal. Feb. 20, 2009).

records and GPS location.[232] Authorities had reason to believe the defendant had kidnapped a child, and contacted the service provider requesting that Sprint voluntarily disclose the information.[233] Two key factors distinguish *Freedman* from *Jayne*. First, the issue at hand in *Jayne* was a cell phone and not an email.[234] The fact that it was a cell phone and that GPS could be used to locate the defendant increases the likelihood of utility and the urgency. Secondly, the authorities only requested the defendant's cell phone records, as it would have been impossible to obtain the content of his communications.[235] These differences tip in the government's favor, and the court approved of the disclosure. The court did not add any caveats, and appeared to completely approve of the voluntary disclosure, but the question remains unanswered as to how a similar case would unfold with an electronic communication.[236]

II. CONNECTING THE CLEAN HANDS DOCTRINE TO THE SCA

The modifications made to Section 2702 of the SCA, particularly the emergency exception, have improved the government's ability to obtain content information from stored communications.[237] This enhanced ability assists in the prevention or detection of a crime, and certainly provides the government with another tool in war on terror.[238] Instead of engaging in the guesswork oftentimes associated with national security prevention, the government may now rely on Providers such as ISPs to monitor communications traveling through their network and alert the government to any potentially catastrophic events. In 2004, the Department of Justice explained the rationale behind the modifications to Section 2702 that have made this possible[239]:

> *Cooperation of Third Parties*
>
> The cooperation of third parties in criminal or terrorist investigations is often crucial to a positive outcome. Third parties, such as telecommunications companies, often can assist law enforcement by providing information in emergency situations. Previous federal law, however, did not expressly allow

[232] *Id*. at *2.
[233] *Id.*
[234] *Id.* at *2,
[235] *Id.*
[236] *Id.* at *7.
[237] *See*, Wayne McCormack, Understanding The Law of Terrorism 135 (2007).
[238] *Id*.
[239] U.S. Dep't of Justice, Report from the Field: The USA PATRIOT Act at Work 26 (2004),*available at* http://www.justice.gov/olp/pdf/patriot_report_from_the_field0704.pdf

> telecommunications companies to disclose customer records or communications in emergencies. Even if a provider believed that it faced an emergency situation in which lives were at risk, if the provider turned over customer information to the government, it risked, in some circumstances, being sued for money damages. Congress remedied this problem in section 212 of the USA PATRIOT Act by allowing electronic communications service providers to disclose records to the government in situations involving an immediate danger of death or serious physical injury to any person. Section 212 has already amply proved its utility.

By enacting Section 2702(b)(8), Congress adapted and codified the policy underpinnings of the "clean hands" exception for surveillance by a third party conducted in violation of Title III. In the name of national security, particularly with respect to the asymmetric nature of the war on terror, Congress has created a provision that not only allows, but encourages ISPs to supply the government with a "lucky break."[240]

This Part first examines some of the similarities between the clean hands exception and the provisions of Section 2702(b)(8). This subsection also briefly touches upon the "grey zone" complication in which ISPs and other telecommunications companies are not sure if a particular set of facts falls within the compulsory disclosure language of Section 2703 or the voluntary disclosure language of Section 2702(b)(8), and the perverse effects this has on government's involvement with potentially dangerous situations. This Part then discusses the deterrent factors influencing each regime, and highlights the failure of Congress to include a reasonable check on ISPs and law enforcement in emergency situations.

A. Assessing Amendments to the Voluntary Disclosure Provisions as Ratifications of the Clean Hands Doctrine

At its core, the clean hands doctrine allows the government to obtain and employ evidence that it either would not be able to obtain on its own, or would not know to obtain on its own.[241] This differs from the good faith doctrine, which essentially allows the government to obtain and employ evidence it knew to and attempted to obtain, but committed a procedural error during the course of

---

[240] *See*, Jim Garamone, *Rumsfeld Says Country Faces Two Options in War on Terror*, American Forces Press Service, August 25, 2003, *available at*http://www.globalsecurity.org/military/library/news/2003/08/mil-030825-afps02.htm (last visited Jan. 17, 2010).

[241] Olsen, s*upra* note 13, at 755.

investigation.[242] The clean hands exception comes at a non-trivial price, as the privacy of an individual—admittedly an individual engaging in illegal behavior—is compromised for the sake of furthering an investigation. While one monitoring the communications of another would likely still face Title III consequences, the doctrine implicitly condones the analysis and subsequent dissemination of this information to government officials.

The similarities between the clean hands exception, which allows the government access to information obtained in violation of Title III, and the emergency provision codified in Section 2702(b)(8), which allows the government access to information voluntarily disclosed by an ISP independent of government compulsion, are numerous. Section 2702(b)(8), much like the clean hands exception—and its predecessor, the good faith exception—avoid the judicially-sanctioned exclusionary rule.

However, there is a key distinction between the two regimes. Those monitoring the activities of others in clean hands cases are still face prosecution for illegally intercepting the electronic communications of another. This provides a deterrent against abuses. This deterrent is not applicable to voluntary disclosures falling under the emergency exception. Voluntary disclosure under the SCA faces three deterrents, though none of them provide enough teeth to satisfactorily deter abuses. First, while there is a civil action remedy available, litigation has been non-existent in cases invoking 2702(b)(8). Secondly, the reporting requirement outlined in Section 2702(d) fails to adequately apply any consequences to abusive monitoring and disclosure. This leaves market forces as the only true impediment to abuses of the voluntary disclosure provisions.

Section 2702(b)(8) provides the government with a similar opportunity to collect and employ evidence that it either was not aware to collect, or potentially was unable to collect through other legal means.[243] For instance, Section 2703 requires the government to obtain a warrant to compel any electronic communication held within 180 days by an ECS.[244] Yet the emergency disclosure provision allows for voluntary disclosure "to a Federal, State, or local governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency."[245] The

---

[242] *See* Part I, supra note xx.
[243] Rosenbloom, *supra* note 7, at 562-63.
[244] 18 U.S.C. 2703(a) (2006).
[245] 18 U.S.C.S. § 2702(b)(8) (2006).

government may be suspicious of an individual, or have reason to suspect harm that falls short of probable cause. In such an instance, the government would not be able to obtain the individual's communications through traditional SCA means. The emergency provision allows the government access to this information completely at the discretion of the Provider. While this may be beneficial in true emergencies, it also opens the door to significant privacy abuses by Providers and the government that are virtually insusceptible to review because of the highly deferential language of the SCA. There are two essential parts to this subsection of the statute, each of which bears comparison with the policy supporting the "clean hands" exception. These are discussed below in turn.

1. The Good Faith Burden and the Exigency of the Situation

In 2006 Congress chose to relax the burden of proof on Providers invoking the emergency disclosure exception.[246] Congress' decision to relax the burden of proof on Providers from a good faith belief for disclosure in emergency situations evidences the government's desire to cast a wide net.[247] This change accomplishes two important goals in encourage proactive compliance by Providers. First, the relaxed standard greatly reduces the likelihood of successful litigation against the Provider.[248] Theoretically a Provider would not have a difficult time demonstrating a good faith fear in an emergency situation in the aftermath of a publicized disclosure. The inclusion of "good faith" avoids complications arising from the inclusion of an immanency requirement, and defers to the Providers' discretion regarding the potential for a situation to develop into an emergency. Secondly, by making the standard so attainable, the government makes the Providers virtually immune from legal liability. As a result, telecommunications companies will be more willing to make disclosures proactively, thereby allowing the government access to maximum information.

Providers face a winless scenario with regard to voluntary disclosure. If they hold on to information that afterward proves to have been capable of preventing a devastating event, public reaction will be negative. Similarly, if telecommunications companies disclose information less judiciously, and the public determines such dissemination to be a violation of privacy, the reaction will again be negative. Such oversight essentially ensures that telecommunications companies will be controlled by public reaction to current levels of concern

[246] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 284-85.

[247] Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135, 2157.

[248] Rosenbloom, *supra* note 7, at 564-65.

regarding terrorism. This encourages a sliding standard of determining imminence with regard to electronic communications.[249]

This winless scenario is similar to the situation the wife in *Murdock* faced for a Title III violation. If she held on to the information, or obeyed the law and never obtained the information, then her husband would have continued to break the law with impunity. Similarly, by revealing the evidence, the defendant's wife opened herself to Title III charges for illegally intercepting private communications. In both cases, the government prefers the interception and divulgence of the information. The executive externalizes the cost of invading individual privacy onto a third party. Under either the clean hands exception or the emergency provision, the government faces less procedural burden by not obtaining a warrant, and does not risk losing the evidence in court over a technicality. If the clean hands exception is applied the technicality of illegally obtained evidence is eliminated per se. Under the emergency exception, the Provider's only burden is that he subjectively believed that harm would occur. Such a standard is almost impossible to dispel. Furthermore, this does not affect the government's case: the remedy for a emergency voluntary disclosure is a civil action, and not exclusion of the evidence.

This incentive broadens when one considers that Providers, as telecommunications companies, will likely be working in tandem with the government in determining the gravity of an imminent threat, as well as identifying the potential targets. Seth Rosenbloom explains:

> Providers are not capable of evaluating the dangerousness of most "emergency" situations without government input. In many cases, the provider's understanding of the "emergency" will rely entirely on the assertions of the same officials who seek disclosure . . . [n]onetheless, the "good faith" standard and absence of an imminence requirement effectively immunize providers. The combination of a lack of reliable information and poor incentives undermines any possibility that providers will adequately check the government's access to information.[250]

Congress' adoption of the "clean hands" policy in its amendments to the SCA is a qualified adoption: voluntary disclosure may only occur in instances threatening danger of death or serious physical injury. This is a natural restriction, given the impetus for amending the

[249] *Id.* at 566.
[250] Rosenbloom, *supra* note 7, at 565.

> statute. The USA PATRIOT Act aims to "deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes."[251]

Congress did not intend to generally broaden the investigative and enforcement powers for less severe circumstances.

The effects cited by the Department of Justice have been less terrorist oriented and more akin to "other purposes". The Department's 2004 Report from the Field concerning the efficacy of the USA PATRIOT Act details one instance in which the emergency language came into play[252]:

> Section 212 was used in the investigation of a bomb threat against a school. An anonymous person, claiming to be a student at a high school, posted on the Internet a disturbing death threat singling out a faculty member and several students to die by bomb and gun. The operator of the Internet site initially resisted disclosing to law enforcement any information about the suspect for fear that he could be sued if he volunteered that information. Once a prosecutor explained that the USA PATRIOT Act created a new provision allowing for the voluntary release of information in emergencies, the owner turned over evidence that led to the timely identification of the individual responsible for the bomb threat. Faced with this evidence, the suspect confessed to making the threats. The operator of the Internet site later revealed that he had been worried for the safety of the students and teachers for several days, and expressed his relief that the USA PATRIOT Act permitted him to help.

This example demonstrates the wide latitude Providers have in determining the exigency of an emergency. While certainly this situation and others profiled in the report merited police intervention, one may question whether they embody the spirit of the USA PATRIOT Act's protection of the United States in the "war on

---

[251] Preamble to the USA PATRIOT Act, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of 18 U.S.C. and 50 U.S.C. (2000 & Supp. 2003)).

[252] U.S. Dep't of Justice, Report from the Field: The USA PATRIOT Act at Work 26 (2004),*available at* http://www.justice.gov/olp/pdf/patriot_report_from_the_field0704.pdf. The report contains a total of five instances in which Section 212 of the USA PATRIOT Act, amending Sections 2702 and 2703 of the SCA, have led law enforcement officials to successful prevention of serious injury. Only the example given could reasonably be categorized as a national security concern.

terror." The undermining of personal privacy is a momentous sacrifice, and flies in the face of the fundamental underpinnings of the Fourth Amendment.[253] As a society we have chosen privacy over the guaranteed prosecution of every crime, preferring individual liberty instead of a "big brother" totalitarian regime.[254]

2. To Whom the ISP May Disclose Information

The *Murdock* court mentioned what it envisions as one effect, or lack thereof, stemming from the admission of a "clean hands" exception: that the government would not feel encouraged to violate privacy protection laws.[255] Inherent in this claim is the idea that if the government had played any part in the illegal surveillance and recording—including merely encouraging a third party to engage in the activity on the government's behalf—the court would invoke the exclusionary doctrine and suppress the evidence.[256] However, such a regime may have unexpected consequences: this could result in widespread private citizen monitoring of one another. Professor Orin Kerr acknowledged such outcome might occur if the "clean hands" doctrine permeated more widely than the Sixth Circuit. He explained that "[i]f the suppression remedy applies only to government misconduct, a private party can make an illegal surreptitious interception of another person's phone call, send it in to the police anonymously, and allow the government to use the evidence against the party whose communication was illegally intercepted."[257]

This could even result in police reliance on third party surveillance. If one envisions the scenario above, in which individuals feel at liberty to monitor the behavior of others, law enforcement officials might become dependent upon the individual surveillance mechanisms, especially given the difficulties and complexities of ascertaining a surveillance warrant.[258] Police burden for obtaining a warrant is high, rife with procedure, and susceptible to judicial whim.[259] As law enforcement become more aware of the clean hands alternative, they may begin to suggest more persuasively that the individuals comply with police insinuations. It is not hard to imagine a scenario in which individuals become conduits for

---

[253] *See* Solove, *supra* note 30, at 1117-28.
[254] *Id.* at 1101.
[255] *Murdock*, 63 F.3d at 1402.
[256] *See, e.g.*, Olsen *supra* note 13, at *756-59.*
[257] Orin Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 Hastings L.J. 805, 837 n. 154 (2003).
[258] *See* Solove, *supra* note 30, at 1119.
[259] *Id.* at 175-76.

investigations lacking in warrants or probably cause, ultimately eroding the protections of the Fourth Amendment.

A similar result is apparent with the modified emergency provision. There is what Professor Orin Kerr calls a "grey zone" in which telecommunications companies will struggle to discern between compelled and voluntary disclosure. In such situations, "government officials have some pre-disclosure contact with providers, but do not 'require' disclosure using the procedures set forth in § 2703."[260] This confusion could lead to an abuse by both law enforcement as well as Providers. *Freedman v. Am. Online, Inc.* evidences the potential for abuse this situation, as the police officers manipulated the ISP to provide information otherwise unattainable.[261]

B. Limitations of Deterrents Under the Emergency Disclosure Provision of the SCA

While the policy underlying the clean hands exception and the emergency disclosure provision of the SCA are very similar in nature, as both allow the government access to information it might otherwise not be aware to investigate or may not be able to investigate, the systemic prevention of abuses in both is very different. Title III still applies to one providing the government information which may eventually escape suppression through the clean hands doctrine. The SCA, however, lacks a substantive and effective means of deterring Providers from overstepping their bounds and interpreting Section 2702(b)(8) broadly. There are three potential factors influencing Providers to exercise discretion in voluntary disclosing personal content information to the government: civil law suits under Section 2707, congressional impugnation after the Department of Justice provides its report pursuant to Section 2702(d), and customer retaliation through market forces.

Section 2707 allows for civil suits against Providers when they violate the SCA with a "knowing or intentional mind."[262] When discussing voluntary emergency disclosure, this language must be paired with the language of Section 2702(b)(8), which allows for a "good faith" belief that an emergency "involving danger of death or serious physical injury" may occur.[263] This combines to mean that a plaintiff must demonstrate that a Provider (1) knowingly or intentionally reported information (2) without a good faith belief that (3) such an emergency

---

[260] Rosenbloom, *supra* note 7, at 565
[261] *Freedman*, 303 F. Supp. 2d at 128.
[262] 18 U.S.C. § 2707(a) (1986).
[263] 18 U.S.C. § 2702(b)(8) (2006).

might occur. This is an almost impossible burden for a plaintiff to carry, and "effectively immunize(s) providers."[264] This is likely the reason that there has been no litigation holding a Provider liable under Section 2702(b)(8).[265] In other words, practitioners understand that the likelihood of success in litigation is virtually zero.[266]

The reporting provision of Section 2702(d) has not been an issue of any litigation to date. While the provision appears to be a check on the Executive Branch through congressional oversight, there are notable limitations on this provision. The most significant limitation is that the provision does not provide for incidents in which information has been disclosed to the government but the investigation has not been closed. There are two possible explanations for this omission. First, this allows the Department of Justice and other national security agencies to continue to monitor potential situations. Secondly, and more cynically, this allows the government to protect an ISP who assisted the government by adhering to the broad disclosure regime in an instance in which disclosure was not reasonable. In either case, this provision is susceptible to manipulation, and does not provide Congress with any ability to remedy abuses. Even if Congress found a Provider to have violated the emergency disclosure provision, the only available remedy lies in civil litigation. Congress would need to convince a judge that the Provider did not subjectively believe that the information was necessary to prevent harm. This is an almost impossible standard for Congress, and leaves the Providers completely insulated.

This leaves customer outrage and market forces as the sole legitimate deterrent to Provider abuses of the emergency disclosure provision. If customers feel that their Provider is abusing their right to privacy, they always have the right to choose another provider. Providers, such as ISPs, have recognized this potential fallout, and many advisors are recommending that they disengage from assisting the government without a search warrant or subpoena. For instance, the U.S. Internet Service Provider Association recognizes the confusion in emergency provision litigation, and recommends taking a safe approach[267]:

> Law enforcement agencies sometimes invoke the "emergency" provision in an effort to avoid the necessity of a subpoena or other process. ISPs often must be firm in pointing out that this provision

[264] Rosenbloom, *supra* note 7, at 565.
[265] Kerr, *The Future of Internet Surveillance Law*, *supra* note 21, at *1209-10.*
[266] *Id.*
[267] U.S. Internet Service Provider Association, *supra* note 183, at 962.

> gives the ISP, not law enforcement, authority to decide whether or not to provide information. There is never an "emergency" obligation on an ISP to disclose under 2702(b)(7) . . . . Because of the intense interest of agencies in this exception, it is prudent for an ISP to adopt clear procedures for its use, and to require all government agencies to adhere to the procedures.

The threat of public embarrassment may be enough to deter abuse of the voluntary disclosure provision, but the jury is still out on this issue. There is of course the threat that failure to disclose information in a true emergency would lead to an equally vociferous backlash if customers believed that the ISP was the only actor capable of prevention.[268] This is potentially the most problematic aspect of the voluntary disclosure deterrence scheme—the reliance on market forces to compel ISP behavior may actually provide *excessive* deterrence, and marginalize the government's ability to obtain the information it truly needs when it needs it. The potential for this outcome was the heart of a letter from Verizon to Congress in 2007, as the general counsel for Verizon explained "placing the onus on the provider to determine whether the government is acting within the scope of its authority would inevitably slow lawful efforts to protect the public" and "would delay the government's receipt of assistance it might need to save lives."[269]

III. APPLYING THE SCA AND CLEAN HANDS TO THE HYPOTHETICALS

The hypotheticals presented at the beginning of this Comment help elucidate the interplay between the clean hands exception and the voluntary emergency disclosure provision of the SCA. The first situation, in which a man has stored on his computer and with an ISP an email containing information vital to his plan to attack a major U.S. city, presents the quintessential case embracing the ISPs' freedom from liability under the SCA. The government does not know about this man, and without the assistance of the ISP, he likely would be able to further his plot with impunity. This constitutes the emergency that we all fear, and the ISP's disclosure of the man's private communications is certainly justified under Section

---

[268] Rosenbloom, *supra* note 7, at 564-65.

[269] Letter from Randal S. Milch, Senior Vice President, Legal & External Affairs & General Counsel, Verizon Business. to John D. Dingell, Chairman, U.S. H.R. Comm. on Energy & Commerce, to Edward J. Markey, Chairman, U.S. H.R. Subcomm. on Telecomm. & Internet, and to Bart Stupak, Chairman, U.S. H.R. Subcomm. on Oversight & Investigations 3-4 (Oct. 12, 2007), *available at* http://markey.house.gov/docs/telecomm/Verizon_wiretaping_response_101207.pdf (last visited April 19, 2010).

2702(b)(8). An individual in possession of such information would, almost assuredly, provide the information to the government notwithstanding the threat of punishment under Title III. In such a situation, the modifications to the emergency disclosure provisions of the SCA play their intended role.

The second scenario, in which a man plots an attack on an individual, is more complicated. There is still an emergency, but it is individual in scope and not within the purview of national security. Furthermore, there is reason to question to reasonable likelihood that the attack will actually occur. The wife in possession of the communication would have to weigh the likelihood of an attack against the potential of her being charged with a Title III offense. The ISP in possession of the same message would likely not face the same consequences—even if the man's plan turned out to be fantasy, it certainly would prevail on the good faith standard. Some might feel that the ISP must or should disclose this information, while others may believe that this does not warrant the invasion of privacy inherent in such disclosure. Such a situation invokes the classic debate over the tradeoff between personal privacy and enhanced police protection—a debate that has consistently fallen on the side of personal privacy before the amendments to the SCA.[270]

The third scenario demonstrates the gravest threat of the emergency provision amendments. The potential for collusive abuse between law enforcement and a third party in possession of information threatens to undermine the entire foundation of personal privacy in communications. The clean hands exception is distinct from the emergency exception in this instance. If a police officer approached an individual for help obtaining the suspect's information, it is almost certain that individual would not comply. The stakes are too high, and there is no demonstrated reason to believe the man is engaged in illegal activity. The threat of collusion is not so overbearing so as to jeopardize the utility of the exception.

A Provider, however, will be more willing to comply. There is no criminal liability associated with an inappropriate disclosure. Further, the deference given to Providers is so great that there is no true threat of civil liability for inappropriate disclosure. Furthermore, the government does not risk losing access to the evidence. This all adds to a situation in which there is no significant legal deterrent to an abuse of the emergency exception. With the only true threat of recourse stemming from customer outrage, the Provider will be willing to work with the police officer provided it was able to satisfy the low burden of good faith in the aftermath. A likely result of this will be a gradual erosion of privacy in communications.

[270] Solove, *supra* note 30, at 1117-28.

CONCLUSION

The voluntary emergency disclosure provisions of the SCA grant a broad degree of discretion to Providers, and allow the government to obtain information it might otherwise be unable to obtain. Like the clean hands exception, this arguably benefits society by allowing law enforcement officials to respond to potential threats in a timely manner. However, the drawbacks of the clean hands exception that similarly exist within the SCA are magnified with the SCA's voluntary disclosure provisions, as these provisions give Providers virtually no incentive, short of customer outrage, to push back against the government's potential abuses. It is likely that in the future, the privacy demands of customers will force Providers to demand the government provide a more robust voluntary disclosure regime so that they feel neither overly nor insignificantly threatened by the ramifications of compliance.

CONTRIBUTORY LIABILITY FOR TRADEMARK COUNTERFEITING IN AN ECOMMERCE WORLD

SCOTT GELIN AND G ROXANNE ELINGS[*]

Scott Gelin and G Roxanne Elings analyze the current standard of contributory liability in the wake of Tiffany (NJ) Inc. v. eBay, in which the Second Circuit affirmed the Southern District's finding that eBay is not liable to trademark owners for counterfeit sales of their products by third parties on its site. After highlighting certain ambiguities in the current state of the law, the authors propose practical tips to help brand owners protect against counterfeit sales, and to help service providers and selling platforms avoid secondary liability.

It has never been easier for sellers of counterfeit goods to avoid getting caught. The Internet is particularly well suited for anonymity, and counterfeiters readily take advantage of the Internet's cloaking abilities. Counterfeiters are able to register domain names, operate web stores that sell counterfeit goods and/or sell counterfeit goods on third party auction platforms, accept and process credit card payments, and ship these illicit goods directly to customers, all without revealing

[*] Scott Gelin is a shareholder in Greenberg Traurig's trademark/brand management group. He counsels clients in a wide variety of IP issues ranging from anti-counterfeiting and brand protection to copyright and trade dress issues. Mr. Gelin represents clients in complex litigation and transactional matters both in the United States and globally. He has significant experience helping clients in the fashion, footwear, luxury goods, beauty products, entertainment and toy industries to protect and enforce their IP rights globally. Mr. Gelin graduated with honors from Cornell Law School and as an undergraduate with honors from Duke University. Outside of his law practice, Mr. Gelin is the Board President of Creative Arts Workshops for Kids (www.caw4kids.org) a not-for-profit which provides free weekend, after school and summer job arts programming to nearly 2,000 underserved children and teens in Northern Manhattan each year.

G Roxanne Elings is a shareholder and co-chair of Greenberg Traurig's trademark/brand management group. She has experience in a full array of brand management issues, including anti-counterfeiting, prevention of grey-market goods and securing and enforcing clients' IP rights. Ms. Eligns has specialized in anti-counterfeiting for 20 years. She obtained the first-ever *ex parte* asset restraint order in an anti-counterfeiting action and was involved in the first efforts by the New York City Mayor's Office to hold landlords liable for counterfeiting on the premises. She has spoken and written extensively in this area. Ms. Elings represents clients in many different industries, including the fashion, luxury goods, fragrance, consumer goods, footwear, interactive gaming and entertainment industries.

their true identities to consumers, who often think they are buying the real thing, or to brand owners who might try to stop them.

But if brand owners cannot catch the actual counterfeiters and make them pay, why not pursue the selling platforms, credit card processors, shippers, and Internet service providers who make these counterfeit sales possible? After all, these entities garner fees when counterfeiters use their services to sell and distribute fake goods. Also, these service providers may know the counterfeiters' true identities and be in the best position to make them stop. Another advantage for brand owners to focus on service providers rather than the counterfeiters themselves is that the former are generally easier to locate and often have deeper pockets.

Service providers, for their part, maintain that the counterfeiting is far removed from the services they provide. They argue that they serve a large number of customers, the vast majority of whom use these services for legitimate purposes, and that they do not have the resources to monitor each customer's use of these services. Service providers also argue that they have no greater knowledge of counterfeiters' true identities than brand owners because counterfeiters provide them with phony names as well. Service providers worry about breaching privacy laws and customer obligations if they provide brand owners with customer information. Some service providers have adopted programs to take down infringing sales and revoke counterfeiters' accounts but wonder why more brand owners are not taking greater advantage of these mechanisms.

Contributory liability in the context of intellectual property infringement is the concept that a service provider can be held responsible for the acts of an infringer for whom it provides services. While the concept of contributory liability for trademark counterfeiting and other intellectual property infringement has been around for decades, it has become an especially vital topic in the age of global ecommerce. This article discusses the current state of contributory liability for trademark counterfeiting against ecommerce service providers and suggests steps, despite the uncertainty in the law, that brand owners can take to persuade third party providers to stop supporting fake sellers, as well as steps service providers can take to avoid liability.

STANDARD FOR CONTRIBUTORY LIABILITY IN TRADEMARK COUNTERFEITING

Contributory liability in the context of intellectual property is governed by the Supreme Court decision *Inwood Labs., Inc. v. Ives Labs., Inc.*,[1] which involved

[1] 456 U.S. 844 (1982).

the sale of generic versions of a prescription drug using the trademark of the original drug. While the pharmacists and not the pharmaceutical companies allegedly used the trademark in question to sell the generic drug, Ives Laboratories, the trademark owner, argued that the generic drug makers were contributorily liable for infringement because they had manufactured the generic drug to resemble the brand-name drug, allowing the pharmacists to pass off the generic drug off as the real thing.[2] The Supreme Court held that the generic drug manufacturers could be liable for contributory infringement if they had either (1) intentionally induced the pharmacists to infringe or (2) supplied these goods when they knew or had reason to know the pharmacists would use them to engage in trademark infringement. The Supreme Court upheld the District Court's findings that Ives Laboratories had not met either standard.[3] The *Inwood* test has since been extended from third-party suppliers of goods to apply to third-party service providers, provided the service providers exercise "direct control and monitoring of the instrumentality" used in the infringement.[4] As a result, flea market or swap meet operators,[5] landlords,[6] check-cashing businesses,[7] and shipping services[8] have all been found liable for trademark counterfeiting by supplying their services to those whom they knew or had reason to know were using these services to commit trademark counterfeiting.

As counterfeiters continue to move their operations from brick-and-mortar stores to the Internet, the new battleground for contributory liability is the extent to which *Inwood* can be applied to ecommerce service providers such as selling platforms, credit card payment processors and Internet service providers. Three recent U.S. cases help focus the parameters of third-party liability in the ecommerce realm.

---

[2] *Id.* at 847.

[3] *Id.* at 854-55.

[4] Lockheed Martin Corp. v. Network Solutions, Inc., 194 F.3d 980, 984 (9th Cir. 1999).

[5] Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996); Hard Rock Café Licensing Corp. v. Concession Services, Inc., 955 F.2d 1143 (7th Cir. 1992).

[6] Cartier Int'l BV v. Ben -Menachem, No. 06 Civ. 3917, 2008 WL 64005 (S.D.N.Y. Jan. 3, 2008); Polo Ralph Lauren Corp. v. Chinatown Gift Shop, 855 F. Supp. 648 (S.D.N.Y. 1994).

[7] Cartier Int'l B. V. v. Liu, No. 02 Civ. 7926(TPG), 2003 WL 1900852 (S.D.N.Y. Apr. 17, 2003).

[8] *Id.*

TIFFANY (NJ) INC. V. EBAY, INC.[9]

The seminal case to set the parameters for contributory infringement in the ecommerce context is *Tiffany (NJ) Inc. v. eBay, Inc.* In 2004, the iconic jewelry brand Tiffany sued eBay, the world's largest on-line selling platform, for contributory liability for trademark counterfeiting, among other claims, based on third-party sales of counterfeit Tiffany jewelry on eBay. Tiffany argued that nearly all Tiffany products sold on eBay were counterfeit, that eBay knew about these counterfeit sales and that it not only refused to stop these sales but actively promoted them since it garnered fees for each sale of these counterfeit products.[10] eBay argued that it is merely an on-line platform that allows third party sellers to list and sell their own products, products which eBay never inspects or comes into contact with. eBay also argued that it had no obligation to halt sales of all Tiffany goods since many were genuine, but that if a particular Tiffany product were suspected to be fake, eBay would promptly remove the sale.[11]

In July 2008, after a bench trial, Judge Richard Sullivan ruled in eBay's favor, finding no liability.[12] The Court found that, contrary to eBay's arguments, eBay exercised direct control and monitoring over sales of counterfeit goods on its selling platform in a way that made it analogous to a swap meet or flea market operator and was thus subject to Tiffany's contributory infringement claim.[13] But the Court held that eBay did not know or have reason to know that all or substantially all Tiffany products being sold on eBay were fake. Indeed, the court found that Tiffany had not established, as it had claimed, that substantially all Tiffany products sold on eBay were fake.[14] The Court found that the Inwood standard did not impose a duty on eBay to anticipate future counterfeit sales but rather a duty to act promptly when it learned that a particular Tiffany product was fake.[15] The Court found that eBay met this standard.

The Court made much about eBay's proprietary "takedown" program called the Verified Rights Owner program ("VeRO"). Under the VeRO program, when a participating brand owner notifies eBay that it has a good faith belief that a particular eBay sale is for a counterfeit version of its products, eBay will remove that listing within twenty-four hours and unwind the sale if it has already been

[9] 576 F. Supp. 2d 463 (S.D.N.Y. 2008).
[10] *Id.* at 494.
[11] *Id.* at 494-95.
[12] *Id.*
[13] *Id.* at 506-507.
[14] *Id.* at 507-10.
[15] *Id.*

effectuated. The Court also noted that eBay employed a staff of 4,000 employees dedicated to fraud prevention, including investigating and stopping the sales of fakes goods on eBay.[16] The Court observed that Tiffany was not taking advantage of eBay's VeRO program to remove sales of fake Tiffany products and encouraged Tiffany to do so.[17]

Tiffany and eBay each appealed parts of the judgment. On April 1, 2010, the Second Circuit upheld the District Court's finding that eBay was not contributorily liable for the sale of counterfeit Tiffany goods on its selling platform.[18] The Second Circuit affirmed the lower court's interpretation of Inwood and its progeny to find that eBay had no duty to anticipate future sales of counterfeit goods on its platform but rather to stop specific sales when it became aware of them and that had eBay met this standard.[19]

LOUIS VUITTON MALLETIER, S.A. V. AKANOC SOLUTIONS INC.[20]

Despite the strong ruling in eBay's favor, the *Tiffany v. eBay* decision did not foreclose the possibility of contributory liability for trademark counterfeiting in the ecommerce context. In another contributory liability case involving ecommerce service providers brought in the United States District Court for the Northern District of California, a federal jury in August 2009 awarded the fashion house Louis Vuitton Malletier $32.4 million in a contributory trademark and copyright infringement action against the Internet service providers Akanoc Solutions, Inc. and Managed Solutions Group, Inc. for failing to shut down a specific group of China-based websites selling counterfeit Louis Vuitton handbags that Defendants had hosted.[21] Louis Vuitton argued that Defendants had direct oversight and monitoring of these web sites that sold counterfeit goods and that it had sent numerous letters to Defendants Akanoc Solutions and Managed Solutions Group putting them on notice of the infringement and demanding that the web sites be taken down, but that Defendants failed to comply. The jury specifically found that Defendants knew or should have known that their customers were engaging in counterfeiting and that they were in a position to stop providing these services but

[16] *Id.* at 478-79.

[17] *Id.*

[18] Tiffany (NJ) Inc. v. eBay, Inc., No. 08-3947-cv2010, U.S. App. LEXIS 6735 (2d Cir. Apr. 1, 2010).

[19] *Id.* at *37.

[20] Verdict, Agreement and Settlement, Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc., 2009 WL 3062893 (N.D.Cal. Aug. 28, 2009).

[21] *Id.* at 9, 13.

did not.[22] The jury found that Defendants had acted willfully[23] and awarded Louis Vuitton the then-maximum statutory damages of $1 million for each of Louis Vuitton's thirteen trademarks, along with maximum copyright statutory damages for various copyrights. In effect, Louis Vuitton was able to satisfy the "know or should have known" prong of the *Inwood* test that Tiffany was unable to show in *Tiffany v. eBay*.

GUCCI AMERICA, INC. V. FRONTLINE PROCESSING CORP.[24]

In another recent action by a brand owner against ecommerce service providers, the U.S. subsidiary of the fashion house Gucci sued three banks and credit card processors last year in the United States District Court for the Southern District of New York for contributory infringement based on the sale of counterfeit Gucci bags. Gucci had brought an action in 2008 against a web store called The Bag Addiction for trademark counterfeiting.[25] Gucci alleged that, in the course of discovery in that action, it learned that Defendants were providing payment processing services for The Bag Addiction while knowing that the web store was selling counterfeit Gucci handbags, and, in fact, were charging higher processing fees because they recognized that there would be more product returns and credit card chargebacks since The Bag Addiction's handbags were counterfeits. The case is currently pending.

PRACTICAL TIPS FOR BRAND OWNERS

Despite the uncertainties about the current parameters of contributory liability against ecommerce providers, brand owners should take advantage of the procedures many service providers have in place to prevent or remove counterfeit sales. One key reason why eBay prevailed in the *Tiffany v. eBay*case because the Court found eBay to have acted promptly to remove listings from its site as soon as it became aware that they might be fake. Given the eBay decision and the jury award in Akanoc, service providers have every incentive to act quickly when they are put on notice of an infringement. While other selling platforms and auction sites might not have as advanced programs as eBay's VeRO program, almost all of them – even the China-based selling platforms – will remove sales identified as fake by brand owners. Many, like eBay's VeRO program, will go further by providing brand owners with the identities of infringing sellers and often prohibit

[22] *Id.* at 7.

[23] *Id.* at 12.

[24] Complaint, Gucci America, Inc. v. Frontline Processing Corp., No. 09-cv-6925 (S.D.N.Y. Aug. 5, 2009).

[25] Gucci Am., Inc. v. Laurette Co., Inc., 08 Civ. 5065 (L.A.K.) (S.D.N.Y. June 3, 2008).

these sellers from using their services again. Some on-line selling platforms will even agree to designate a brand name or trademark as a "forbidden" term so that sellers cannot use that term to list or describe their goods. In addition to online selling platforms, other ecommerce service providers like Internet service providers, web hosts, search engines that sell sponsored adwords and payment processors will remove listings and stop providing service upon notice of an infringement.

Brand owners should set up a system to send "takedown" notices to various selling platforms on a daily basis. These takedown efforts are a cost-effective way to remove vast numbers of fake goods from the market each month, which may discourage counterfeiters altogether, or at least force them to move on to less enforced brands. Moreover, the information gathered from takedown programs can be used to identify the larger counterfeiters and the most valuable litigation targets. In the event brand owners do not receive compliance from a service provider, the brand owner's takedown and compliance efforts may help build a case for contributory infringement like Louis Vuitton did in Akanoc.

PRACTICAL TIPS FOR SERVICE PROVIDERS

Despite the uncertainties in contributory infringement for ecommerce service providers, it is important for service providers to be aware of the factors involved in proving contributory liability and to stay on the right side of them. The *Tiffany v. eBay* opinion provides the clearest roadmap to date for how a service provider can avoid liability – essentially by adopting all of the enforcement policies that Judge Sullivan commended eBay for adopting. The biggest factor seems to be whether action is taken when a service provider is put on notice of infringement. While both eBay and the Defendants in Akanoc were found to have been in a position to exercise direct control and monitoring over the infringing activities, eBay was found to have acted promptly to remove sales and stop providing services while the Akanoc Defendants were found to have intentionally continued providing services after this notice was given. Service providers should have systems in place to remove users who are selling infringing products or using their services to sell infringing goods. Service providers should make sure their posted "terms of use" and agreements with customers clearly prohibit use of their services for counterfeiting and allow them to revoke users and provide the users' information to authorities or the brand owner.

STUDENT-ATHLETES AND THE NCAA: PLAYING BY THE RULES

STEVEN OLENICK*

When student-athletes seek representation or advisement to evaluate post-collegiate playing opportunities, their eligibility may be in jeopardy. Steven Olenick suggests a checks and balance system to truly evaluate post-collegiate playing opportunities for students.

Prized basketball recruit Renaldo Sidney has yet to step foot on the court for the Mississippi State Bulldogs. His eligibility status remains uncertain due to an ongoing investigation by the National Collegiate Athletic Association (NCAA) into his amateurism status regarding receiving improper benefits.[1] Oklahoma State star wide receiver, Dez Bryant, was ruled ineligible by the NCAA this past season for lying about a meeting with NFL great Deion Sanders.[2] Major League Baseball prospect Andrew Oliver was suspended by Oklahoma State University because he had violated Bylaw 12.3.1 by allowing his former attorney to contact a Major League club and by having his former attorney present when a Major League Baseball club tendered him a contract.[3] Recently, another Major League Baseball

* Steven Olenick is an Associate in the Entertainment, Media & Publishing, Advertising, Marketing & Promotions and Intellectual Property Groups of Davis & Gilbert. He counsels individuals, entertainers, current and retired professional athletes, coaches, start-ups, sports agencies, marketing companies, advertising companies and digital media companies in connection with all aspects of advertising, marketing, digital technology and sports and entertainment. In addition, Mr. Olenick counsels and provides strategic business advice to current and retired professional athletes and sports agencies all over the world.

Prior to joining the firm, Mr. Olenick worked for Entersport Management, Inc, an agency that specializes in the representation of professional basketball players internationally. Mr. Olenick began his legal career at Paul, Weiss, Rifkind, Wharton & Garrison LLP, a firm widely recognized as a leader in litigation and corporate transactions.

[1] Mike DeCourcy, *Attorney: Mississippi State Mishandling Renardo Sidney's Eligibility*, Sporting News, Jan. 8, 2010. http://www.sportingnews.com/college-basketball/article/2010-01-08/attorney-mississippi-state-mishandling-renardo-sidneys-eligibi

[2] Thayer Evans, Oklahoma State Declares Star Receiver Bryant Ineligible, N.Y. Times, Oct. 8, 2009 at B17, also available at http://www.nytimes.com/2009/10/08/sports/ncaafootball/08bryant.html.

[3] Division I Agents, Amateurism and Elite Student-Athletes, http://web1.ncaa.org/web_files/regional_seminars/2009/DI/Outlines/DI%20Agents,%20Ama%20and%20ESA%20OL.pdf (Last visited Mar. 25, 2010). *See also*

prospect, James Paxton, had his eligibility questioned for his dealings with a Major League Baseball club.[4]

One theme remains constant in all of these aforementioned matters: student-athlete amateurism status. Under the NCAA Bylaw's, any student-athlete will be ruled ineligible in any collegiate sports if he or she has committed themselves verbally or in writing to be represented by an agent.[5] The NCAA furthers their stance by not allowing a student-athlete to enter into a representation agreement verbally or in writing until after the student-athlete has completed their eligibility.[6] The NCAA's position is intended to keep professionals away from student-athletes.[7] The NCAA is not directly prohibiting student-athletes from engaging professionals, such as attorneys, so long as they do not have direct contact with professional teams.[8] The NCAA carries out these bylaws by requiring student-athletes to sign a non-negotiable waiver which bars them from competing in intercollegiate sports in the event that they do not sign the form. Although this may appear to be a constitutional violation, depriving a student-athlete of his or her Fourteenth Amendment due process right, the NCAA's conduct is not actionable under state law when a private organization does not adopt state rules, but, rather, holds collective membership within a private organization.[9]

So where does this leave potential professional prospects needing proper guidance in the agent selection process and player contract negotiation? The NCAA does not prohibit hiring an attorney or business manager; however, neither can represent the student-athlete openly during negotiations with a professional team.[10] Attorneys and business managers can discuss the merits of a deal with a student-athlete and guide him or her appropriately throughout the agent selection process, however, at no time may they initiate discussions between the team and player, nor directly contact the team on the player's behalf.[11] This anachronistic approach by the NCAA may appear to monopolize student-athletes. History

---

http://www.ncaa.org/wps/wcm/connect/34a376804e0b88ef937ef31ad6fc8b25/AgentBrochure.pdf?MOD=AJPERES&CACHEID=34a376804e0b88ef937ef31ad6fc8b25 (Last visited Mar. 25, 2010).

[4] *See id.*

[5] *See id.*

[6] *See id.*

[7] *See id.*

[8] *See id.*

[9] *See* NCAA v. Tarkanian, 488 U.S. 179 (1988).

[10] *See id*. *See also* Pitt's Blair Declares for NBA Draft, http://sports.espn.go.com/nba/draft2009/news/story?id=4052755 (last visited Mar. 26, 2010).

[11] *Id.*

suggests that the NCAA does not want anyone to challenge its loosely worded bylaws pertaining to agent legislation.[12] Additionally, the paucity of case law suggests that the NCAA is very sensitive in resolving any matter attacking these specific bylaws to uphold its existing form.

One possible panacea would be to strongly encourage the NCAA to work in concert with all governing professional sports leagues to ensure that student-athletes who have the ability to play post-college have access to a checks and balance system that would provide them with proper guidance in evaluating a post-collegiate career. The NCAA determines whether schools have proper oversight and compliance, but it can be argued that their bylaws may be widely interpreted. The NCAA is intended to protect student-athletes and provide them the best opportunity to succeed both on and off the court. Unfortunately, however, for the few select student-athletes that have the ability to extend their career beyond the collegiate ranks, the NCAA could be limiting their ability to obtain proper guidance and receive credible information that could sway their decision making process. By modifying the NCAA bylaws to allow for the NCAA to become the mediator between the potential professional prospect and the professional team, the NCAA could monitor the discussions and obtain the proper information to pass along to the student-athlete for him or her to decide on his or her potential professional future. Additionally, implementing an effective checks and balance approach would allow student-athletes to receive proper oversight during the decision making process and allow for the NCAA to provide the much needed oversight currently lacking in student-athlete decision making. Until the NCAA introduces alternative measures to minimize the lack of oversight and information relayed to student-athletes, student-athletes will not be able to obtain proper guidance to help them through the difficult decision making process of declaring for professional drafts or foregoing collegiate eligibility.

---

[12] Rendall Rogers, *Report: Kentucky Ace Pitcher James Paxton Sues School*, Destination: Omaha, Dec. 3, 2009, http://rivals.yahoo.com/ncaa/baseball/blog/ncaabb_experts/post/Report-Kentucky-ace-pitcher-James-Paxton-sues-s?urn=ncaabb,206373. *See also* Liz Mullen, *OSU P Andy Oliver Files Suit Against NCAA, Former Advisor*, SportsBusiness Journal, July 2, 2008, http://www.sportsbusinessdaily.com/article/122046.