



United States District Court,
D. Kansas.

UNITED STATES of America, Plaintiff,
v.
Michael R. KENNEDY, Defendant.

No. 99-10105-01.

Jan. 3, 2000.

Defendant, who was indicted for the intentional receipt of child pornography, filed motion to suppress evidence. The District Court, Belot, J., held that: (1) even if Internet service provider divulged defendant's subscriber information pursuant to a court order based on an inadequate government application, suppression was not a remedy contemplated under Electronic Communications Privacy Act (ECPA); (2) defendant did not have a Fourth Amendment privacy interest in his Internet subscriber information; (3) even if the government's attainment of defendant's subscriber information from Internet service provider violated the Cable Communications Policy Act (CCPA), statute afforded him no suppression remedy; and (4) searches of defendant's computer files by anonymous caller and Internet service provider personnel was not subject to Fourth Amendment.

Motion denied.

West Headnotes

[1] Telecommunications **514.1**
[372k514.1 Most Cited Cases](#)

Government's application for a court order, which merely listed that subscriber information connected to certain Internet service provider address would possibly relate to an on-going criminal investigation, did not meet the requirements of Electronic Communications Privacy Act (ECPA); government should have articulated more specific facts such as how the government obtained the information it did have at the time and how this information lead the agents to believe that the attainment of the subscriber information of that particular Internet service provider address would assist in the investigation. [18 U.S.C.A. § 2703\(d\)](#).

[2] Criminal Law **394.1(2)**
[110k394.1\(2\) Most Cited Cases](#)

Even if Internet service provider divulged defendant's subscriber information pursuant to a court order based on an inadequate government application, suppression was not a remedy contemplated under Electronic Communications Privacy Act (ECPA). [18 U.S.C.A. § 2701](#) et seq.

[3] Searches and Seizures **26**
[349k26 Most Cited Cases](#)

Defendant did not have a Fourth Amendment privacy interest in his Internet subscriber information; when defendant entered into an agreement with provider for Internet service, he knowing revealed all information connected to his subscriber address. [U.S.C.A. Const.Amend. 4](#).

[4] Criminal Law **394.1(2)**
[110k394.1\(2\) Most Cited Cases](#)

Even if the government's attainment of defendant's subscriber information from Internet service provider violated the Cable Communications Policy Act (CCPA), statute afforded him no suppression remedy. Communications Act of 1934, § 631(f), as amended, [47 U.S.C.A. § 551\(f\)](#).

[5] Searches and Seizures **33**
[349k33 Most Cited Cases](#)

Fourth Amendment's protection against unreasonable searches and seizures proscribes only governmental action; it is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official. [U.S.C.A. Const.Amend. 4](#).

[6] Searches and Seizures **33**
[349k33 Most Cited Cases](#)

Private search will be deemed governmental for Fourth Amendment purposes only when government knew of and acquiesced in the intrusive conduct, and party performing the search intended to assist law enforcement efforts rather than to further his own ends. [U.S.C.A. Const.Amend 4](#).

[7] Searches and Seizures **33**
[349k33 Most Cited Cases](#)

Searches of defendant's computer files by anonymous caller and Internet service provider personnel was not

subject to Fourth Amendment since government did not either know of or acquiesce in either the private searches. [U.S.C.A. Const.Amend. 4.](#)

[8] Searches and Seizures  **113.1**
[349k113.1 Most Cited Cases](#)

An affidavit in support of a search warrant must provide a substantial basis for determining the existence of probable cause; that there is a fair probability that evidence of a crime will be found in the place to be searched. [U.S.C.A. Const.Amend. 4.](#)

[9] Searches and Seizures  **113.1**
[349k113.1 Most Cited Cases](#)

Mere fact an affidavit does not contain personal knowledge of illegal activity at the residence is not fatal to the determination of probable cause to search. [U.S.C.A. Const.Amend. 4.](#)

[10] Searches and Seizures  **116**
[349k116 Most Cited Cases](#)

Special agent's affidavit in support of the government's application for a search warrant, which relied on the hearsay testimony of anonymous caller and Internet service provider personnel to establish that defendant possessed child pornography on his computer's hard drive, was sufficient to establish probable cause to search defendant's computer files where agent stated enough corroborating evidence from his observations of defendant's house and his pretext phone call placed to defendant; the "informants" were not of the "criminal milieu" for purposes of assessing their veracity. [U.S.C.A. Const.Amend. 4.](#)

[11] Criminal Law  **1130(6)**
[110k1130\(6\) Most Cited Cases](#)

Fact that a defendant's argument is first made in his reply brief does not prevent the court from considering the issue.

[12] Criminal Law  **412.2(3)**
[110k412.2\(3\) Most Cited Cases](#)

Police officers are not required to administer *Miranda* warnings to everyone whom they question; instead, the warnings mandated by *Miranda* apply only to statements obtained from an individual who is subjected to custodial police interrogation.

[13] Criminal Law  **412.2(2)**

[110k412.2\(2\) Most Cited Cases](#)

Question to ask when determining whether custody existed at the time of police questioning, for purposes of requiring *Miranda* warnings, is simply whether there is a formal arrest or restraint on the freedom of movement of the degree associated with a formal arrest; standard to be used in asking that question is whether a reasonable person in the suspect's position would have understood his situation as the functional equivalent of formal arrest.

[14] Criminal Law  **412.2(2)**
[110k412.2\(2\) Most Cited Cases](#)

Police interview of defendant was not a custodial interrogation and therefore agents were not required to inform defendant of his rights under *Miranda*; interview occurred in defendant's home, in the afternoon, after defendant invited the agents in, defendant was never handcuffed and neither agent exhibited any sign of force, defendant never asked for an attorney and he never refused to answer a question, and the interview lasted only twenty to thirty minutes.

[15] Criminal Law  **519(1)**
[110k519\(1\) Most Cited Cases](#)

Whether a confession is coerced depends upon several factors: (1) the age, intelligence, and education of the defendant; (2) the length of the detention; (3) the length and nature of the questioning; (4) whether the defendant was advised of his constitutional rights; and (5) whether the defendant was subjected to physical punishment. [18 U.S.C.A. § 3501.](#)

[16] Criminal Law  **531(3)**
[110k531\(3\) Most Cited Cases](#)

In view of lack of any evidence presented on defendant's susceptibility to coercion, the short duration of the interview, the non-coercive environment in which the interview was conducted and the fact that defendant was never threatened, defendant's confession was voluntary.

***1105** [Debra L. Barnett](#), Office of United States Attorney, Wichita, KS, for plaintiff.

[Daniel E. Monnat](#), Monnat & Spurrier, Chartered, Wichita, KS, for defendant.

MEMORANDUM AND ORDER

BELOT, District Judge.

On August 25, 1999, Defendant Michael R. Kennedy was indicted for the intentional receipt of child pornography in violation *1106 of 18 U.S.C. § 2252(a)(2) (Doc. 1) and forfeiture under 18 U.S.C. § 2253. Before the court for its consideration are:

1. Defendant's motion to suppress evidence (Doc. 13);
2. Defendant's memorandum in support of his motion to suppress (Doc. 14) [FN1];

[FN1]. In his supporting memorandum, defendant states that "[t]he lack of argument in this brief on some allegations of the defendant's Motion to Suppress is not a waiver of any such allegations ..." (Doc. 14 at 1). Not so. Failure to press a point by supporting it with pertinent authority forfeits the point. See Phillips v. Calhoun, 956 F.2d 949, 953-54 (10th Cir.1992).

3. The government's response (Doc. 20);
4. The government's memorandum in support of its response (Doc. 21); and
5. Defendant's reply (Doc. 22),

An evidentiary hearing was held December 2, 1999. For the following reasons, defendant's motion to suppress is denied.

FACTS

On July 2, 1999, Steven Idelman was working as a customer support specialist for Road Runner, a high speed Internet service provider. [FN2] At approximately 9:00 p.m., Idelman received an anonymous phone call from a still- unidentified male ("the caller"). The caller told Idelman that he was at a friend's house, scanning other computers through the Internet and had viewed images of child pornography on a computer the caller believed to be serviced by Road Runner. The caller told Idelman the IP address of the computer from which the images were viewed, 24.94.200.54, [FN3] and the directory and file names in which the images were located. [FN4] The caller did not say that he was a law enforcement officer or that he was directed to view the computer's files by any law enforcement officer. The caller did not ask Idelman to call the police.

[FN2]. Road Runner High Speed Online is a division of Multimedia Cablevision, Inc.

Road Runner is a participant in the trend of providing Internet services over two-way, interactive broadband systems owned by cable companies. See generally, Barbara Esbin, Internet Over Cable: Defining the Future in Terms of the Past, 7 CommLaw Conspectus 37, 89-94 (1999) (discussing Internet technology provided over cable systems).

[FN3]. The IP, or Internet Protocol, address is unique to a specific computer. Only one computer would be assigned a particular IP address. See Espin, supra at 46-47 (discussing Internet Protocols).

[FN4]. The caller was able to view the computer's files because the computer with IP address 24.94.200.54 had its print and file sharing mechanism turned on, allowing other computers to view its files over the Internet.

Shortly after the anonymous call, Idelman went to a computer and accessed the IP address given to him by the caller. His purpose was to determine if what the caller told him was correct. He located the computer with the IP address 24.94.200.54 and the directory tree and files mentioned by the caller. Idelman viewed two images located within those files. One of the images depicted two boys, whom Idelman estimated to be approximately eight or nine years old, posed in a sexual nature. [FN5] Idelman then sent an e-mail to his supervisor, Anna Madden, describing the anonymous phone call and the results of his search of the computer with IP address 24.94.200.54.

[FN5]. At the evidentiary hearing, Idelman could not recall specifically the image in the second file. He could only testify that he remembered it being in the nature of child pornography.

On July 6, 1999, Kerry Jones, a network engineer for Road Runner, received an e-mail from Anna Madden asking him to research the owner of the Road Runner account connecting to the computer with the IP address 24.94.200.54. Jones was able to determine that the account was *1107 assigned to Rosemary D. Kennedy. [FN6] Mr. Jones was able to determine

that the account was assigned to the same IP address on July 2, 1999. Believing that the customer service agreement between Road Runner and the account holder authorized him to search a computer's files for offensive material, Jones then viewed the files on the computer's hard drive. [\[FN7\]](#) The files depicted images of boys, whom Jones estimated to be approximately 10 to 13 years old, engaged in sexual activity. Jones then printed out an image of the computer's directory tree in which the files with offensive material were located.

[FN6.](#) Road Runner misidentified the account holder as "Rosemay."

[FN7.](#) Jones was able to do so because the computer's print and file sharing mechanism was still turned on.

That same day, after consulting with Road Runner's corporate attorney, Scott Petrie, the manager of Road Runner, made the decision to contact law enforcement authorities. Kerry Jones contacted the Exploited Children's Unit of the Wichita Police Department, but his phone call was not returned. Road Runner then contacted Special Agent Leslie Earl of the FBI. Special Agent Earl was informed by Road Runner that the FBI would need to obtain a court order for it to be able to supply the FBI with any subscriber information.

The United States Attorney's Office then applied to a United States magistrate judge for an order directing Road Runner to disclose subscriber information related to IP address 24.94.200.54. In the application, the Assistant United States Attorney stated that:

the Federal Bureau of Investigation is conducting a criminal investigation in connection with possible violation(s) of Title [18, United States Code, Sections 2252](#) and [2252A](#); it is believed that the subject of the investigation used Road Runner's IP address 24.94.200.54 on July 2, 1999, at 11:48 p.m. in furtherance of the subject offenses; and that the information sought to be obtained is relevant to a legitimate law enforcement inquiry in that it is believed that this information will assist in the investigation relating to the aforementioned offenses.

The magistrate judge issued an order, which was presented to Road Runner personnel, who provided the FBI with the following information:

The subscriber whose computer used I.P. address 24.94.200.54 on July 2, 1999, at 11:49 p.m. was Rosemay (sic) D. Kennedy of 9120 Harvest Court, Wichita, Kansas, telephone 316-722-6593. Two users were listed for that account: RKENNEDY@KSCable.COM and KENNEDYM@KSCable.Com. The account had been active since June 7, 1999.

Special Agent Earl next went to the house located at 9120 Harvest Court in Wichita, Kansas. He observed a Chrysler Sebring parked in the driveway. A records check with the Kansas Department of Motor Vehicles revealed that the car was registered to Michael R. Kennedy. Special Agent Earl then called the phone number given to the government by Road Runner. A person identifying himself as Michael Kennedy answered the phone.

In initiating the phone call, Special Agent Earl asked Kennedy if he was satisfied with his Road Runner cable modem Internet service.

Kennedy confirmed that his address was 9120 Harvest Court, Wichita, Kansas, and he confirmed that he was the primary user of the Road Runner cable modem Internet service. Kennedy said he was satisfied with the service and especially liked the speed and quality of the e-mail service. Kennedy estimated he spent an average of two to three hours per night online. Kennedy noted that he always left his system on and connected to the Internet. Kennedy said he used his Internet access only for *1108 pleasure and his computer and modem were located in his home.

Kennedy said his computer system was a Gateway 450 megahertz Pentium II with a 17 gigabyte hard drive. When asked if he had any concerns about the Road Runner service Kennedy said he thought the company should warn customers about the possibility of someone else trying to enter their computers through the Internet. Kennedy said he held Internet accounts through Netcom and AOL in the past. Kennedy left those services because they were too slow and he could not use e-mail and Usenet news groups the way he wanted to. Kennedy noted that it took too long for him to download mail with pictures attached on those other services.

(Affidavit in Support of Search Warrant at 14-15, Doc. 14, Ex. A). The government applied for and obtained a search warrant for property and evidence located at 9120 Harvest Court.

On August 10, 1999, Special Agents John Sullivan and Leslie Earl went to defendant's home to interview

him and execute the search warrant. When defendant came to the door, the agents identified themselves. Defendant invited them in and the three men sat down in the kitchen. During the interview, defendant's mother and brother were in the living room, watching television.

Special Agent Sullivan told defendant why they were interviewing him. Defendant was informed that he was not under arrest and that he would not be arrested at the end of the interview. After providing the agents with some identifying information, defendant stated that he was 46 years old, did not have any drug or alcohol addiction problems, that he was not at that time under the influence of drugs or alcohol, and that he was not being treated for any physical or psychological problems. Defendant told the agents that he had spent one year in college.

Defendant stated that he owned three computers and used Multimedia Cablevision as his Internet service provider. Defendant acknowledged that he had downloaded pictures of young boys engaged in sexual acts from the Internet onto his hard drive. Defendant told the agents that he did not pay for any of the pictures, he did not know the identity of the person who posted the pictures on the Internet, he never discussed the pictures with anyone, nor had he ever transferred the pictures to anyone else. Defendant denied ever using an Internet chat room and claimed he never had any sexual contact with anyone under the age of 18. Although defendant admitted hearing that the possession of sexually explicit pictures of children was illegal, he was not really sure about the legality. Defendant stated that he did not think that anyone would ever find out that he had downloaded the pictures.

Defendant then showed the agents four sexually graphic pictures of young boys that he had printed out. These pictures were in defendant's bedroom. Defendant showed the agents his computers in the basement.

The interview lasted twenty to thirty minutes. Defendant never raised the issue of an attorney. Defendant never refused to answer a question. The agents never promised defendant anything in return for his statements. Defendant was not arrested at the conclusion of the interview and was allowed to turn himself in after the return of the indictment.

ANALYSIS

A. SUBSCRIBER INFORMATION RECEIVED FROM ROAD RUNNER

Defendant first argues the subscriber information the FBI received from Road Runner should be suppressed. Defendant argues that the information was received in violation of the Electronic Communications Privacy Act and the Cable Communications Policy Act. Defendant further argues that all evidence obtained as a result of the illegal attainment of defendant's *1109 subscriber information should be suppressed as fruit of the poisonous tree. Although the court finds that the ECPA was violated, suppression of the evidence is not a remedy for such a violation. Because suppression is likewise not a remedy provided for under the CCPA, the court need not determine whether or not that statute was implicated.

1. *The Electronic Communications Privacy Act*

[1] [18 U.S.C. § § 2701 et seq.](#) regulates the disclosure of electronic communications and subscriber information. [Section 2703\(c\)\(1\)\(B\)](#) states that "[a] provider of electronic communication service ... shall disclose a record or other information pertaining to a subscriber to or customer of such service ... to a governmental entity only when the governmental entity ... (ii) obtains a court order for such disclosure under subsection (d) of this section." Subsection (d) sets forth the requirements of such a court order:

(d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) ... shall issue only if the governmental entity offers *specific and articulable facts* showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

[18 U.S.C. § 2703\(d\)](#) (emphasis added).

Defendant argues the government's application did not state specific and articulable facts, but mere conclusions. The government responds that at the time of the application, it did not know the identity of the subscriber, whether the subscriber was the person using the computer to store illegal material and how much child pornography was held by the computer. The government argues that the information it had at the time was minimal and the purpose of obtaining the order was to investigate the subscriber information completely.

The government's argument does not address the issue as to conclusory versus specific and articulable facts in regard to the information it *did* have. The government's application merely listed that the

subscriber information connected to IP address 24.94.200.54 would possibly relate to an on-going criminal investigation. [\[FN8\]](#) In accordance with [18 U.S.C. § 2703\(d\)](#), the government should have articulated more specific facts such as how the government obtained the information it did have at the time and how this information lead the agents to believe that the attainment of the subscriber information of this particular *1110 IP address would assist in the investigation. The government's application for a [section 2703\(d\)](#) order did not meet the requirements of the statute.

[FN8](#). It appears as though the government's application would have satisfied the statute's requirements prior to the 1994 amendments to the ECPA. As the statute was originally enacted, the government's application for the court order sufficed by showing there was reason to believe the information sought was "relevant to a legitimate law enforcement inquiry." Electronic Communications Privacy Act, [Pub.L. No. 99-508 § 201, 1986 U.S.C.A.A.N. \(100 Stat.\) 1862](#). In the early 1990's, a task force, assembled by Senator Patrick Leahy "questioned whether current restrictions on government access to transactional records generated in the course of electronic communications were adequate." H.R.Rep. no. 103-827, at 12 (1994), *reprinted in* 1994 U.S.C.A.A.N. 3489, 3492. In response, the statute was amended to its current version. *See* Communications Assistance for Law Enforcement Act, [Pub.L. No. 103-414 § 207\(2\), 1992 U.S.C.A.A.N. \(108 Stat.\) 4292](#). The House Report reflects that [t]his section imposes an intermediate standard to protect on-line transactional records. It is a standard higher than a subpoena, but not a probable cause warrant. The intent of raising the standard for access to transactional data is to guard against "fishing expeditions" by law enforcement. Under the intermediate standard, the court must find, *based on law enforcement's showing of facts, that there are specific and articulable grounds to believe that the records are relevant and material to an ongoing criminal investigation*. H.R.Rep. No. 103-827, at 31-32 (1994), *reprinted in* 1994 U.S.C.A.A.N. 3489, 3511-12 (emphasis added).

[\[2\]](#) Nonetheless, the government correctly points out that even if Road Runner divulged defendant's subscriber information pursuant to a court order based on an inadequate government application, suppression is not a remedy contemplated under the ECPA. The statute specifically allows for civil damages and criminal punishment for violations of the ECPA, *see* [18 U.S.C. § § 2707, 2701\(b\)](#), but speaks nothing about the suppression of information in a court proceeding. [\[FN9\]](#) *Compare* [18 U.S.C. § 2515](#) (prohibiting the use of communications intercepted in violation of Title III of the Omnibus Crime Control and Safe Streets Act as evidence in any trial). Instead, Congress clearly intended for suppression not to be an option for a defendant whose electronic communications have been intercepted in violation of the ECPA. The statute specifically states that "[t]he remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter." [18 U.S.C. § 2708](#).

[FN9](#). The court does not suggest that defendant has a civil remedy. On the contrary, [18 U.S.C. § 2703\(e\)](#) specifically precludes a civil action when the service provider gives information pursuant to a court order.

[\[3\]](#) Defendant's constitutional rights were not violated when Road Runner divulged his subscriber information to the government. Defendant has not demonstrated an objectively reasonable legitimate expectation of privacy in his subscriber information. On the contrary, the evidence is that defendant's computer had its sharing mechanism turned on. The only reasonable inference is that defendant had done so. *See* [California v. Greenwood, 486 U.S. 35, 39, 108 S.Ct. 1625, 1628, 100 L.Ed.2d 30 \(1988\)](#). "[W]hat a person knowingly exposes to the public, even in his home or office, is not a subject of Fourth Amendment protection." [Katz v. United States, 389 U.S. 347, 351, 88 S.Ct. 507, 511, 19 L.Ed.2d 576 \(1967\)](#). "[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." [Smith v. Maryland, 442 U.S. 735, 743-44, 99 S.Ct. 2577, 2582, 61 L.Ed.2d 220 \(1979\)](#). When defendant entered into an agreement with Road Runner for Internet service, he knowing revealed all information connected to the IP address 24.94.200.54. He cannot now claim to have a Fourth Amendment privacy interest in his subscriber information.

2. *The Cable Communications Policy Act*

Defendant argues that the Cable Communications Policy Act, not the Electronic Communications Privacy Act, is the controlling statute which establishes the procedures for an Internet service provider, such as Road Runner, to disclose to the government a subscriber's information. The CCPA mandates the service provider notify the subscriber before divulging information to the government. Defendant contends that the government's attainment of the information was in violation of the CCPA and should be suppressed. The government responds that the CCPA does not apply.

In 1984, Congress enacted the CCPA to establish guidelines for the cable industry and set forth "a nationwide standard for the privacy protection of cable subscribers." H.R.Rep. No. 98-934, pt. IV, at 76 (1984) *reprinted in* 1984 U.S.C.A.N. 4655, 4713. The Act is codified at [47 U.S.C. § § 251 et seq. Section 551](#) provides a privately enforceable scheme designed to protect cable subscriber privacy. This section regulates the disbursement of "personally identifiable information." [\[FN10\]](#) *1111 The Act specifically states that, before obtaining information about a cable subscriber from a cable operator, the government must apply for a court order and offer clear and convincing evidence that the subscriber is suspected of engaging in criminal activity and that the information sought would be material evidence in the case. *See* [47 U.S.C. § 551\(h\)](#). [\[FN11\]](#) Furthermore, the CCPA requires that the subject of the information sought by the government must be notified and given the opportunity to contest the government's claim. *See* [§ 551\(h\)\(2\)](#).

[FN10](#). The legislative history of the CCPA notes that such information "would include specific information about the subscriber, or a list of names and addresses on which the subscriber is included." H.R.Rep. No. 934, pt. IV at 79, *reprinted in* 1984 U.S.C.A.A.N. 4655, 4716. The court finds that the information regarding defendant which was given to the government was such personally identifiable information.

[FN11](#). The court finds the requirements for the government's application for such a court order more stringent than those necessary for an order under the Electronic Communications Privacy Act. Thus, it may

be assumed that if the government's application did not meet the standards under the ECPA, it was not sufficient under the Cable Communications Policy Act.

Traditionally, Internet providers have considered themselves subject to the regulations and prohibitions set forth in the Electronic Communications Privacy Act. *See, e.g., United States v. Hambrick*, [55 F.Supp.2d 504, 507 \(W.D.Va.1999\)](#) (analyzing Internet service's providing of customer's information under the ECPA). Cable operators, however, are subject to the Cable Communications Policy Act. So where does a cable operator, providing Internet services, look for its regulatory scheme? [\[FN12\]](#) In this case, did Road Runner, a provider of high speed Internet services over cable wires, by complying with the Electronic Communications Privacy Act, completely identify and comply with its statutory duties?

[FN12](#). [47 U.S.C. § 522\(5\)](#) defines cable operator as "any person or group of persons (A) who provides cable service over a cable system...." Subsection (6) defines cable service as "(B) subscriber interaction, if any, which is required for the selection *or use* of such video programming or other programming service." In 1996, the CCPA was amended to include the words "or use." The House Conference Report states that "[t]he conferees intend[ed] the amendment to reflect the evolution of cable to include interactive services such as game channels and information services made available to subscribers by the cable operator, as well as enhanced services." *See* H.R.Conf.Rep. No. 104-458, at 169 (1996) *reprinted in* 1996 U.S.C.A.A.N. 124, 182.

The issue of whether the CCPA applies to a company such as Road Runner is one of first impression. Only one district court has discussed the issue. *See In re United States of America*, [36 F.Supp.2d 430 \(D.Mass.1999\)](#). In *In re United States*, the issue was raised in an application for an order under the Electronic Communications Privacy Act. *See id. at 431*. The district court was able to avoid deciding the statutory conflict by concluding it lacked jurisdiction because the issue was not ripe for adjudication. *See id. at 433*.

[\[4\]](#) This court need not decide whether the CCPA

was violated in the instant action because even if it were, defendant still would not be entitled to suppression of the evidence as a remedy for the violation. As with the ECPA, the CCPA speaks nothing of an exclusionary remedy, only a civil remedy. See [47 U.S.C. § 551\(f\)](#). Furthermore, for the same reasons defendant did not have a Fourth Amendment interest under the ECPA, he has no such interest under the CCPA. See also, [Scofield v. Telecab of Overland Park, Inc.](#), [973 F.2d 874, 876-77 \(10th Cir.1992\)](#) ("[The notice requirements of section 551] do not themselves create a class of protected privacy interests. That is, subscribers have no privacy interest in receiving a notice itself."). Therefore, even if the government's attainment of defendant's subscriber information from Road Runner violated the Cable Communications Policy Act, the statute affords him no suppression remedy.

B. INITIAL SEARCHES OF DEFENDANT'S COMPUTER FILES

Defendant argues that the initial warrantless searches of his computer files *1112 were done by government actors and were therefore in violation of his Fourth Amendment rights. The searches he refers to are those performed by the anonymous caller and Road Runner personnel. He asks this court to suppress all evidence as fruit of this poisonous tree. Because the court finds that these searches were done entirely by private individuals, the searches were not within the purview of the Fourth Amendment.

[\[5\]\[6\]](#) The Fourth Amendment's protection against unreasonable searches and seizures "proscribe[s] only governmental action; it is wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.'" [United States v. Jacobsen](#), [466 U.S. 109, 113, 104 S.Ct. 1652, 1656, 80 L.Ed.2d 85 \(1984\)](#) (quoting [Walter v. United States](#), [447 U.S. 649, 662, 100 S.Ct. 2395, 2404, 65 L.Ed.2d 410 \(1980\)](#) (Blackmun, J., dissenting)). The Tenth Circuit applies a two part test in determining when a search by a private individual becomes government action: "1) whether the government knew of and acquiesced in the intrusive conduct, and 2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends." [Pleasant v. Lovell](#), [876 F.2d 787, 797 \(10th Cir.1989\)](#). Both inquiries must be answered in the affirmative before an otherwise private search will be deemed governmental for Fourth Amendment

purposes. See [United States v. Leffall](#), [82 F.3d 343, 347 \(10th Cir.1996\)](#).

[\[7\]](#) In this case, the first requirement is not met. There is no evidence to support defendant's allegation that the government either knew of or acquiesced in either the caller's or the Road Runner personnel's search of defendant's computer. "The proponent of a motion to suppress bears the burden of proof." [United States v. Madrid](#), [30 F.3d 1269, 1275 \(10th Cir.1994\)](#). Defendant bears the burden of establishing that the government involvement of the initial searches was significant enough to change them into governmental searches. Defendant has not met his burden. [\[FN13\]](#)

[FN13.](#) At the December 2 hearing, defendant's counsel extensively cross-examined Road Runner employees in an attempt to establish or impute some law enforcement connection to their activities. In addition, he subpoenaed David Flemming, Multimedia Inc.'s vice-president and general counsel, for the same purpose. Counsel wholly failed in his attempt. No evidence was developed which even hinted at a law enforcement connection.

C. AFFIDAVIT IN SUPPORT OF THE SEARCH WARRANT

Defendant next argues Special Agent Earl's affidavit in support of the government's application for a search warrant failed to establish probable cause. The search warrant, he continues, was therefore defective and all evidence seized as a result of the search warrant should be suppressed along with defendant's confession as fruit of the poisonous tree. Defendant argues that because the affidavit relies on the hearsay testimony of the anonymous caller and Road Runner personnel to establish that defendant possessed child pornography on his computer's hard drive, and because these "informants" were of the "criminal milieu", a neutral and detached magistrate could not have made an independent determination about the veracity of the informants and could not have determined that probable cause existed.

[\[8\]\[9\]](#) " 'An affidavit in support of a search warrant must provide a substantial basis for determining the existence of probable cause; that there is a fair probability that evidence of a crime will be found in the place to be searched.' " [United States v. Richardson](#), [86 F.3d 1537, 1545 \(10th Cir.1996\)](#)

(quoting *Massachusetts v. Upton*, 466 U.S. 727, 732-33, 104 S.Ct. 2085, 2087-88, 80 L.Ed.2d 721 (1984)). "The mere fact an affidavit does not contain personal knowledge of illegal activity *1113 at the residence is not fatal to the determination of probable cause." *United States v. Parrish*, 925 F.2d 1293, 1296 (10th Cir.1991). In determining whether an affidavit states sufficient probable cause, the magistrate must rest on a common-sense, practical look at the totality of the circumstances. See *Upton*, 466 U.S. at 732, 104 S.Ct. at 2087-88. A magistrate's determination is to be paid "great deference" by a reviewing court. See *United States v. Martinez*, 764 F.2d 744, 746 (10th Cir.1985) (quoting *Illinois v. Gates*, 462 U.S. 213, 236, 103 S.Ct. 2317, 2331, 76 L.Ed.2d 527 (1983)).

[10] Defendant's argument relies on Road Runner's search of his computer files being in violation of *Kan.Stat. Ann. § 21-3755*, the Kansas state crime of computer trespass. Defendant repeatedly contends that Road Runner's employees were "criminals", [FN14] and therefore the magistrate judge should have discounted their statements and asked for more corroborating evidence in order to find probable cause. For this proposition, defendant cites Wayne R. LaFave's treatise, *Search and Seizure*, as stating "[c]ourts are much more concerned with veracity when the source of the information is an informant from the criminal milieu rather than an average citizen who has found himself in the position of a crime victim or witness." Wayne R. LaFave, *Search and Seizure* § 3.4 at 204 (3d ed.1994). The court, however, finds that it need not delve into an interpretation of Kansas's criminal trespass statute or the customer service agreement between defendant and Road Runner, as defendant suggests, in order to determine that Road Runner's personnel were average citizens and not the "criminal milieu" spoken of by Professor LaFave.

[FN14]. Doc. 14 at 11 and 17-18; Doc. 22 at 5. The court finds it ironic that defense counsel, who considers himself a champion of the rights of defendants, would label Road Runner's employees as "criminals." There is no evidence that Road Runner's employees have been investigated for or charged with a violation of *K.S.A. 21-3755*, much less convicted. Counsel would express outrage if this court disregarded the presumption of innocence and referred to defendant as a "criminal." Surely counsel should extend the same presumption to persons who have not even been charged with a crime.

A more thorough reading or quotation of the treatise would reveal that the distinction made by the courts Professor LaFave speaks of is between "citizen-informers," who report crimes out of concern for society, and the traditional police informer, exchanging information for some concession or payment. See *id.* at 204-24. All evidence points to Road Runner's employees being informers of the former type, not the latter. No evidence suggests that Road Runner's employees offered to give the government defendant's name in exchange for getting them off the hook for an impending state prosecution for computer trespass. Whether a defendant can comb the state criminal statute books looking for some applicable statute has no bearing on the citizen informer's characterization. Indeed, the words "criminal milieu" conjure up images of shady drug dealers and car thieves lurking in dark corners, turning over names in interrogation rooms to save their own skin. Surely Professor LaFave meant not to include within the definition the computer engineer who policed his employer's system for child pornography. [FN15]

[FN15]. The court need not review the reliability and veracity afforded to the anonymous caller. The caller never contacted police. The caller was not an informant and any discussion of the caller in Special Agent Earl's affidavit was merely as background information for purposes of establishing the Road Runner employees' knowledge.

Furthermore, the affidavit stated enough corroborating evidence to support a finding of probable cause based on Road Runner's tip. The affidavit before the magistrate judge listed not only Special Agent Earl's expertise in the area of child pornography and the Internet, but also what Special Agent Earl had learned from *1114 Road Runner personnel and the corroborating facts obtained from the phone call placed to defendant. Looking at the affidavit under the totality of circumstances, the magistrate judge had a reasonable basis to believe probable cause existed.

Although Special Agent Earl's phone call revealed nothing more than innocent activity on the part of defendant, the information gained was enough corroborating information for the purpose of establishing probable cause. See *United States v.*

Brown, 984 F.2d 1074, 1076-77 (10th Cir.1993) (quoting Illinois v. Gates, 462 U.S. 213, 238, 103 S.Ct. 2317, 2332, 76 L.Ed.2d 527 (1983)). In Brown, an unnamed informant told a prosecutor that defendants were in possession of stolen vehicles. See Brown, 984 F.2d at 1075. A police detective later observed defendants dismantling a car in the front yard of the house mentioned by the informant. See id. at 1076. The Tenth Circuit found that the "seemingly innocent activity" of working in a partially dismantled truck became suspicious in light of the informant's tip. See id. at 1077. The court stated that the corroborating information gave the magistrate judge a "substantial basis for crediting the hearsay" included in the tip." Id. (quoting Gates, 462 U.S. at 244-45, 103 S.Ct. at 2335).

In this case, the affiant, Special Agent Earl, stated enough corroborating evidence from his observations of defendant's house and his pretext phone call placed to defendant. During the phone call, defendant told Special Agent Earl he was the primary user of the Internet service, he was worried that other people were reading his computer's files through the Internet, and that he liked to download pictures from the Internet. This otherwise innocent activity corroborated the tip received from Road Runner that defendant had child pornography located in his computer files.

[11] In his reply brief, defendant also argues that the affidavit for search warrant failed to state any factual information supporting the Road Runner technician's conclusion that the images on defendant's hard drive were children under the age of eighteen. [FN16] The cases cited by defendant relate to testimony of witnesses at trial and whether such testimony could be admitted as either lay or expert testimony. These cases have no bearing on what evidence may be considered by the magistrate in determining if probable cause exists. The court finds that the magistrate had sufficient evidence before him to conclude there was probable cause that the pictures seen by Road Runner personnel were of children under the age of eighteen.

[FN16] The fact that defendant's argument is first made in his reply brief does not prevent the court from considering the issue. See United States v. Palmer, 604 F.2d 64, 66 (10th Cir.1979).

D. DEFENDANT'S STATEMENTS ON AUGUST 10TH

1. Custodial Interrogation

Defendant next argues that his statements to Special Agents Sullivan and Earl should be suppressed because the agents never advised him of his rights under Miranda. The government concedes the agents never told defendant of his Miranda rights but insists that such was not required because defendant was not, at that time, under arrest and the interview was not the equivalent of a custodial interrogation. The court agrees.

[12][13] "[P]olice officers are not required to administer Miranda warnings to everyone whom they question." Oregon v. Mathiason, 429 U.S. 492, 495, 97 S.Ct. 711, 714, 50 L.Ed.2d 714 (1977 (per curiam)). Instead, the warnings mandated by Miranda apply only to "statements obtained from an individual who is subjected to custodial police interrogation." Miranda v. Arizona, 384 U.S. 436, 439, 86 S.Ct. 1602, 1609, 16 L.Ed.2d 694 (1966). The question to ask when determining whether *1115 custody existed at the time of police questioning "is simply whether there is a 'formal arrest or restraint on the freedom of movement' of the degree associated with a formal arrest." California v. Beheler, 463 U.S. 1121, 1125, 103 S.Ct. 3517, 3520, 77 L.Ed.2d 1275 (1983) (per curiam) (quoting Mathiason, 429 U.S. at 495, 97 S.Ct. at 714). The standard to be used in asking this question is whether a reasonable person in the suspect's position would have understood his situation as the functional equivalent of formal arrest. See United States v. Glover, 104 F.3d 1570, 1578 (10th Cir.1997). The court's inquiry should focus on the totality of the circumstances and is fact intensive. See id.

[14] The agents' interview of defendant occurred in defendant's home, in the afternoon, after defendant invited the agents in. See United States v. Erving L., 147 F.3d 1240, 1247 (10th Cir.1998); United States v. Ritchie, 35 F.3d 1477, 1485 (10th Cir.1994) ("[C]ourts are much less likely to find the circumstances custodial when the interrogation occurs in familiar or at least neutral surroundings, such as the suspect's home.") (internal quotation omitted). Defendant was told he was not under arrest and that he would not be arrested at the conclusion of the interview. See Erving L., 147 F.3d at 1247; Glover, 104 F.3d at 1579. Defendant was never handcuffed and neither agent exhibited any sign of force. See id. Defendant never asked for an attorney and he never refused to answer a question. See id. the interview lasted only twenty to thirty minutes. See United States v. Benally, 146 F.3d

[1232, 1239 \(10th Cir.1998\)](#). Under the totality of the circumstances, the court finds that the interview of defendant was not a custodial interrogation and the agents' failure to inform defendant of his rights under *Miranda* does not require suppression of his statements.

2. *Voluntariness of Defendant's Confession*

[\[15\]\[16\]](#) Defendant finally argues his statements at the August 10th interview should be suppressed because it was not voluntary. Whether a confession is coerced depends upon several factors: (1) the age, intelligence, and education of the defendant; (2) the length of the detention; (3) the length and nature of the questioning; (4) whether the defendant was advised of his constitutional rights; and (5) whether the defendant was subjected to physical punishment. See *Schnecko v. Bustamonte*, 412 U.S. 218, 226, 93 S.Ct. 2041, 2047, 36 L.Ed.2d 854 (1973); *Glover*, 104 F.3d at 1579. See also 18 U.S.C. § 3501 (listing factors to be considered by the court in determining voluntariness of confession). Based on the totality of the circumstances, see *id.*, the court finds that defendant's confession was voluntarily given and was not coerced. This finding is based on the lack of any evidence presented on defendant's susceptibility to coercion, the short duration of the interview, the non-coercive environment in which the interview was conducted and the fact that defendant was never threatened. See *Benally*, 146 F.3d at 1240. Defendant's confession was voluntary and will not be suppressed.

CONCLUSION

IT IS THEREFORE ORDERED BY THE COURT that defendant's motion to suppress (Doc. 13) is DENIED.

IT IS SO ORDERED.

81 F.Supp.2d 1103

END OF DOCUMENT