UIC John Marshall Journal of Information Technology & Privacy Law

Volume 22
Issue 4 *Journal of Computer & Information Law - Summer 2004*

Article 2

Summer 2004

The States and the Electronic Communications Privacy Act: The Need for Legal Processes That Keep Up With the Times, 22 J. Marshall J. Computer & Info. L. 695 (2004)

Monique Mattei Ferraro

THE STATES AND THE ELECTRONIC COMMUNICATIONS PRIVACY ACT: THE NEED FOR LEGAL PROCESSES THAT KEEP UP WITH THE TIMES

MONIQUE MATTEI FERRARO†

I. INTRODUCTION

Put yourself in the position of a local police officer for just a few moments. Your dispatcher assigns you to respond to a call. A mother complains that her daughter is missing. The child is twelve, and has not returned home since she left for school at 6:30 this morning. It is now midnight, and the girl's mother is at her wit's end.

You arrive at the complainant's home. It's beautiful. The town where you work has a low crime rate, and the average income of the residents is respectable. You approach the door knowing that this call might resolve itself uneventfully and happily, or it could be heart-wrenching and tragic. You bolster yourself for the greeting because you will set the tone for the rest of this crisis.

You knock on the door, and almost as soon as your fist reaches the door, the girl's mother whips it open. "Thank God you're here!" she bursts. "My little girl is in trouble. I know it!"

"Ma'am, please calm down," you say. "I need to get some information from you and in order to ensure that we are able to do the best we can to get your daughter home safely, you must remain calm. We need you to be calm so that you can give us as much information as you can so that we can locate her and bring her home safely."

"All I know is that she left for school this morning and she never came home."

"Was she supposed to go somewhere after school? A friend's house?"

---

† M.S., Northeastern University; J.D. University of Connecticut School of Law 1998, Certified Information Systems Security Professional. The author advises the State of Connecticut Department of Public Safety, Computer Crimes and Electronic Evidence Unit/Internet Crimes Against Children Task Force. Her book, *Investigating Child Exploitation and Pornography: The Internet, the Law and Forensic Science*, co-authored with Eoghan Casey will be published in September 2004.

"She was supposed to be at cheerleading practice," the mother says. Her eyes begin to fill with tears, but she regains her composure. You need her to be all business. "When she left school she didn't get on the bus. She didn't meet the parent who was driving to cheerleading, either. Sometimes I pick her up and take her to practice on my own, so the other parent wasn't concerned."

"I'll need to talk to that parent," you say.

"Certainly, whatever you need," the mother offers. "She is a very close friend and she's very eager to help."

"She isn't a suspect at this point. We'll need to talk with everyone with relevant information at this point," you say. (You might be a novice, but you have seen enough TV movies to know the routine.)

You continue with the scripted questions, and then you touch upon a hot topic. "Does she have a boyfriend or frequently use the Internet?"

"Oh, my God," the mother gasps. She hadn't thought of the Internet connection until now. "She's always on the Internet, to the point where we have threatened to stop our Internet service! She's online all the time, talking to who-knows-who at God-knows-what hours of the day and night! She gets telephone calls from people I have never heard of, and she even gets things in the mail from them. I even found PANTIES one time that she was sending someone! Can you imagine? A twelve-year-old girl sending panties in the mail?"

Aha! Now you have a solid lead. The girl's online communications will lead you to her. Maybe she's safe. She may be following an online relationship with someone who genuinely cares for her and may have her best interests at heart. More often than we would like to think, she may be the victim of an online sexual predator, and she may be dead by now. Time could be of the essence, or not. Twelve year-old girls run away all the time. They also forget to call home to tell their parents that they are staying at a friend's house, and sometimes they stay away from home for other reasons. At this point, there simply is not enough information to draw any conclusions.

Knowing what we all know from all of the detective shows and legal training we have received, what does the patrol officer do next?

Anybody? . . . .

Anybody? . . . .

Beuller? . . . .

Beuller? . . . .

Well, the first thing the officer should do, besides covering herself by telling her supervisor what's going on and getting permission to proceed, is to get permission from the girl's parents to access her computer and Internet service. At this point, the girl is not suspected of any criminal conduct.

The officer goes to the girl's computer and accesses her Internet account.[1] She finds correspondence and logged chat and instant messages that lead her to believe that the child left home to meet someone with the screen name of "imsowilling73" that same day at a location in the town where the girl resides.

The next step is to find out who "imsowilling73" is. But how? You call the service provider and, after your call is transferred several times, you get the number for their legal process division. Luckily, they have a 24/7 number (most ISPs do not), but you wait on hold for twenty minutes before someone answers. When a representative answers, he tells you to "get a subpoena, fax it to us and we'll fax back the information."

"Huh?" you say. You never heard of such a thing. You call your supervisor. He, in turn, calls the local prosecutor. She hasn't heard of such a thing, either. Now what? You call the service provider again. This time you have the direct number for the legal process division.

"Fax us a court order or a search warrant, and we'll fax you back the information," the representative tells you.

You call your local prosecutor and tell her what the ISP told you. She says she has never heard of a court order for that type of thing, and no judge in your state would sign a search warrant for information held outside of your state. Now what?

When hours can mean the difference between successful resolution of a case or not, law enforcement has to have a streamlined and effective method of obtaining necessary information. But, even though it has been nearly twenty years since its passage, the Electronic Communications Privacy Act ("ECPA")[2] still confuses state and local law enforce-

1. For purposes of this article, we will ignore the forensic consequences of accessing an Internet service account at the scene by the investigating officer.

2. 18 U.S.C. § 2703 provides:

(a) Contents of wire or electronic communications in electronic storage. A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of wire or electronic communications in a remote computing service.

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records concerning electronic communication service or remote computing service.

(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure; or

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for court order. A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and 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. In the case of a State governmental

ment. As more and more criminal activity has an online nexus, local and state law enforcement is thrust into an esoteric area of the law in which little accurate guidance can be found.

This article will take the reader on a tour of the cybercrime investigator's landscape.

The article begins with an overview of the ECPA, followed by a multifaceted explanation of the problem. It concludes with discussion of possible solutions.

II. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")

The ECPA sets out the process for the government to obtain information held by Internet service providers[3] ("ISPs"). The ECPA mandates that the government use certain minimal legal process to obtain the information they seek. The type of legal process is dictated by how long the information has been held in storage and the type of information sought.

We dispense with the length-of-storage distinction. For all practical purposes, the way that ISPs operate and the way that crimes and investigations develop translate into state and local law enforcement only requiring data in storage less than one hundred eighty days.[4] Presently,

---

authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No cause of action against a provider disclosing information under this chapter. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter [18 USCS §§ 2701 et seq.].

(f) Requirement to preserve evidence.

(1) In general. A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention. Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) Presence of officer not required. Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter [18 USCS §§ 2701 et seq.] requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

3. The ECPA also applies to compelling production of information held by telephone companies about their subscribers, but for ease of discussion, this article confines the discussion to ISPs.

4. 18 U.S.C § 2703(a) (2004).

the ECPA authorizes three methods for obtaining information from electronic communications service providers:

1. administrative, grand jury or trial subpoena;
2. a court order issued pursuant to 18 U.S.C. §2703(d); or
3. a search warrant.[5]

The less privacy protection afforded to the type of record, the less intrusive the legal process required. For instance, in order to obtain subscriber information, that is, the record of who subscribes to an Internet access account, including the person's name, address and credit card used to establish the account, the police need only issue a subpoena. In order to obtain transaction data such as when an individual accessed her account, what services she used and how long she was online, the police must obtain a court order. Similar to real time communication, in order to obtain the content of stored communications, police must obtain a search warrant.[6]

Congress enacted the ECPA for several reasons, but mainly they wanted to protect ISPs from liability for releasing information about their customers to the government. They also wanted to establish a level of privacy in Internet records and communications to avoid inevitable legal battles over the issue.[7] The liability issue is obvious. The protection against liability is similar to other provisions of the federal law that limit liability of communications providers relative to providing assistance with wiretaps, pen registers and trap and trace captures.

The data protected by the ECPA is held by third parties.[8] If not for the ECPA, there would be no barrier to prevent police from asking for any records held by ISPs. The United States Supreme Court addressed

5. Subtle distinctions dictating the process prescribed for information depending upon whether the information has been held in electronic storage more or less than 180 days are not addressed here for ease of discussion, but for particular application of the statute, the amount of time information has been held in storage will impact the process.

6. 18 U.S.C. § 2510 et seq.; *See also Katz v. U.S.*, 389 U.S. 347 (1967).

7. Sen. Rep. 99-541 (1986); 132 Cong. Rec. S14441 (1986).

8. The statute creates the privacy protection provided to Internet records and communication. The information the statute protects is not necessarily protected under the Fourth Amendment against unreasonable search and seizure. As the United States Supreme Court held in *Smith v. Md.*, 442 U.S. 735 (1979), one does not have either an objective or subjective expectation of privacy in the information they readily hand over to a third party.

In *Smith*, the telephone company installed a device called a "pen register" on Smith's telephone line at police request. A pen register is a device that captures the telephone numbers dialed from a telephone line. At trial, Smith moved to suppress evidence obtained from the pen register, arguing that police needed a search warrant. The trial court denied the motion, holding that no warrant was required as the Fourth Amendment was not implicated. The Maryland Court of Appeals affirmed, as did the United States Supreme Court. The U.S. Supreme Court held that Smith could not claim either a subjective expectation of privacy or that such a belief was one society would be prepared to recognize as "reasonable."

the issue directly in *Smith v. Maryland,*[9] holding that one cannot have an expectation of privacy in information willingly handed over to a third party. In order to afford privacy protection to data held by ISPs, Congress enacted the ECPA. While Congress had good intentions when it enacted the ECPA, the states have been mired in confusion since its passage. The following discusses three areas that cause the greatest angst.

III. THE STATES AND THE ECPA—ALMOST SQUEEZING A SQUARE PEG INTO A ROUND HOLE

A. THE ECPA PROVIDES FOR COMPULSORY PROCESS THAT ARE ALIEN TO STATE AND LOCAL LAW ENFORCEMENT

Compared to federal authorities, state and local jurisdictions are hamstrung when it comes to investigative tools to combat cybercrimes and crimes with an online nexus. Most states do not authorize administrative subpoenas. States that allow for grand jury subpoenas often limit the authority to certain crimes or felonies, or the grand jury may not always be in session. Trial subpoenas are almost irrelevant because the main use of subpoenas in cybercrime investigations is to obtain subscriber information, which is mostly used at the initial stages of an inquiry to identify potential suspects.

Even in jurisdictions where authorities can use subpoenas to obtain subscriber information, questions over jurisdiction can be a factor. State jurisdiction is limited by their long-arm statutes.[10] While many states have long-arm statutes that allow the state to exercise jurisdiction to the extent that the United States Constitution allows,[11] others do not. As a result, even if a state allows subpoenas for Internet subscriber information, if the state's long-arm statute does not permit it, a different method to compel production of the information must be used.

Jurisdictions that do not allow subpoenas force police to attempt to use more complicated procedures that take more time and may not work at all. The next higher form of process from a subpoena is the § 2703(d) order. The ECPA provides that state courts may issue § 2703(d) orders, but only if state law does not prohibit issuing the orders. As with subpoenas, state court orders do not have any force beyond the jurisdiction of

---

9. *Id.*

10. *See* Robert C. Casad, *Long Arm and Convenient Forum*, 20 U. Kan. L. Rev. 1 (1971); David P. Currie, *The Growth of the Long Arm: Eight Years of Extended Jurisdiction in Illinois*, 1963 U. Ill. L. Forum 533 (1963); Cal. Civ. Proc. Code § 410.10; *Restatement (Second) of Conflict of Law* § 37 (2004).

11. California's long-arm statute, for example. The first long-arm statutes were enacted to enable civil suits against foreign corporations and out-of-state drivers who could not be personally served in the state, Eugene Scoles & Peter Hay, *Conflict of Laws* § 8.2 (2d ed., 1992).

the issuing court. So the order is only good in another jurisdiction if the state's long-arm statute allows it and is constitutionally permissible. For the most part, an ISP will have sufficient contacts with the forum state to justify obtaining jurisdiction in accordance with constitutional due process.[12]

In reality, state and local authorities rarely use court orders to obtain ISP information. Investigators say that if they must "articulate facts" sufficient to support a § 2703(d) order that they may as well swear an affidavit for a search warrant because there is usually probable cause to support the warrant. In fact, in many jurisdictions the process for obtaining a court order would be more cumbersome than obtaining a search warrant. Lack of familiarity with § 2703(d) orders also prevents state officials from seeking them. Government attorneys and judges who have never seen a § 2703(d) order application require explanation, and generally need time to conduct their own research before they feel comfortable going forward.

1. *How federal authorities do it*

At the federal level, obtaining evidence from ISPs is fairly straightforward. Many federal agents can issue subpoenas requesting the production of Internet service subscriber information. If an agent cannot issue a subpoena on her own, she has ready access to an Assistant United States Attorney who can issue a subpoena. Administrative subpoenas and grand jury subpoenas do not require supporting affidavits or judicial authorization.

Obtaining a 2703(d) order is a similarly simple matter.

> [T]he governmental entity [must] offer [ ] 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.[13]

Federal § 2703(d) orders issued by one District are valid in another.[14] This is a major distinction from state court orders that may or may not be valid in another state.

Federal search warrants for content information are also straightforward. A search warrant issued by the District with jurisdiction over

12. *International Shoe*, 326 U.S. 310 (1945); *World-Wide Volkswagen Corp v. Woodson*, 444 U.S. 286 (1980); *Burger King v. Rudzewicz*, 471 U.S. 462 (1985).

13. 18 U.S.C. § 2703(d).

14. This is a recently added provision of the law, courtesy of the *PATRIOT Act*. Prior to the Act, the § 2703(d) order had to be obtained in the jurisdiction in which the ISP was located. Pub. L. No. 107-56, Title II, §§ 209(2), 210, 212(b)(1), 220(a)(1), 220(b), 115 Stat. 283, 285, 291, 292 (Oct. 26, 2001).

the offense is valid in the District where the records are held.[15] The federal search warrant statute also allows agents to request the assistance of civilians to carry out the search,[16] and the federal law "does not require the presence of law enforcement when service providers collect and produce information pursuant to a search warrant because the problems associated with private exercise of search and seizure powers are not implicated when service providers collect and produce information in response to a warrant."[17]

Federal authorities enjoy other advantages over state and local law enforcement when they seek information from ISPs. Federal law enforcement has centralized administration. Policies and procedures for using investigative tools are issued by the central authority and are common to all of the components. There are vast resources for training[18] and the Department of Justice has the Computer Crimes and Intellectual Property Section ("CCIPS") dedicated to assisting agents and United States Government attorneys. CCIPS compiled frequently cited guidelines for search and seizure of computers and digital evidence.[19] However, federal training and CCIPS guidelines are not intended to address the needs of the States or the individual nuances that distinguish state from federal law.

2. *All 50 States are Different (AKA: Federal Law v. State Law)*

For the states, the process for obtaining information from ISPs can be lengthy, and the legal process the investigating officer must use can be quite complex. First, the officer must figure out what ISP is the carrier of the account related to the evidence sought. The initial identifying information may be an e-mail address, an IP address, a website uniform resource locator ("URL") or other. There are thousands of Internet service providers located throughout the United States and abroad. Once an officer identifies the ISP, he needs to identify the contact information for the service provider. Once the contact information has been identified, the officer will contact the ISP to determine how the company prefers to receive the compulsory process.

15. 18 U.S.C. § 2703(a).

16. "A search warrant may in all cases be served by any of the officers mentioned in its direction or by an officer authorized by law to serve such warrant, but by no other person, except in aid of the officer on his requiring it, he being present and acting in its execution." 18 U.S.C. § 3105.

17. 18 U.S.C. § 3105.

18. For instance, the Federal Law Enforcement Training Center ("FLETC") in Georgia, the National White Collar Crime Center, the FBI National Academy in Quantico, VA to name only a few.

19. *Computer Crimes and Intellectual Property Section, United States Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, at III.D.3 (July 2002).

As a practical matter, police officers investigating a crime are more interested in actually obtaining the information they seek in an expeditious manner. Often, state and local investigators will duplicate efforts by doing what the ISP wants them to do and doing whatever their supervisors, government attorneys or judges tell them they need to do to satisfy local requirements.

This article began with an example. Neither the police officer nor the prosecutor in the case knew what to do to get the information they needed in order to resolve the case. Unfortunately, at the state and local levels, this is the rule rather than the exception.

B. Execution of State Search Warrants

There are a few problems associated with search warrants for out-of-state information held by ISPs. First, for some jurisdictions the only method available to obtain simple Internet account subscriber information is a state search warrant. Second, jurisdiction of state courts is questionable, and confusing at the very least, when it comes to issuing search warrants for information held outside of the borders of the state. This issue is complicated by full faith and credit statutes. Finally, when a state court issues a search warrant for ISP information held out-of-state, the warrant will most likely be executed by non-police personnel who work for the ISP. This practice conflicts with many state statutes that direct police to execute the search. The relevant issues will be discussed in turn.

1. *When a "Man" is Sent to Do a "Boy's Job": Forcing States to Use a Search Warrant for Simple Subscriber Information*

At least two practical issues arise when state and local police must obtain a search warrant for basic subscriber information. First, police may only need subscriber information even though they have sufficient probable cause to justify a search warrant.

The purpose of the ECPA is to protect our privacy. Even though police usually have sufficient probable cause to justify a search warrant for ISP held information, they do not always need all the information they may lawfully obtain. Ideally, the least intrusive legal process available should be used in order to protect individuals' privacy. For subscriber information, the least intrusive legal process is a subpoena. A search warrant authorizes the police to conduct a search for evidence. Despite the ECPA provision that states, "the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter,"[20] state search warrants often direct an officer

20. 18 U.S.C. § 2703(g).

to conduct the search.[21]

Second, when a search warrant is required, the jurisdiction where the ISP is located may be unwilling or unable to assist. For example, a police officer in a jurisdiction that forces him to obtain a search warrant for ISP subscriber information (Officer John) calls the police department with jurisdiction over the ISP to request that they obtain a search warrant for him. The police officer with jurisdiction (Officer Jane) tells John that because the ISP is located in California, he is in luck because all he has to do is fax his state warrant to the ISP, and they will provide him with the necessary records. If the local judge will not sign John's warrant and the police department in California will not get a warrant for him and execute it, then, John and his investigation are at a dead end.

2. *What Jurisdiction Should Obtain the Warrant and "Full Faith and Credit" Statutes*

The proper procedure for one state to obtain a search warrant and execute a search in another state is to solicit the assistance of the law enforcement agency with physical jurisdiction over the ISP. Using information from the requesting state, the state with jurisdiction applies for a search warrant and executes it at the ISP. Two factors complicate this process. First, three states—California, Minnesota and Florida—have statutes that recognize the validity of search warrants for ISP information.

California, Minnesota and Florida have statutes that recognize the validity of search warrants for information held by ISPs.[22] These statutes direct ISPs within their states to produce information requested by the out-of-state search warrant. The out-of-state police officer is expected to fax or mail the search warrant to the ISP.

---

21. Connecticut, for example. C.G.S. § 54-33 (2004).

> The warrant shall be directed to any police officer of a regularly organized police department or any state policeman or to a conservation officer, special conservation officer or patrolman [ ]. The warrant shall state the date and time of its issuance and the grounds or probable cause for its issuance and shall command the officer to search within a reasonable time the person, place or thing named, for the property specified.

C.G.S. § 54-33a(c). New York's statute states:

> A search warrant must contain: 1. The name of the issuing court and, except where the search warrant has been obtained on an oral application, the subscription of the issuing judge; and 2. Where the search warrant has been obtained on an oral application, it shall so indicate and shall state the name of the issuing judge and the time and date on which such judge directed its issuance. 3. The name, department or classification of the police officer [ ] to whom it is addressed.

NY CLS CPL § 690.45 (2003). *See also U.S. v. Bach*, *infra* n. 25.

22. Cal. Penal Code §1524.2 (2003), Fla. Stat. § 92.605 (2003) and Minn. Stat. § 626.18 (2003).

For many jurisdictions, this eases the burden both of locating a contact in the police department with jurisdiction and of clearing many administrative hurdles. A problem that has emerged is that some judges absolutely will not sign search warrants that will be executed outside of their jurisdiction. Even after the affiants produce the California, Minnesota or Florida statute, there are judges who continue to refuse to authorize the search. An officer faced with this usually has to let the investigation go because when he requests assistance from the state with jurisdiction, they tell him to get a search warrant from his state. Another issue that arises out of the full faith and credit statutes is where police should file the return on the search warrant execution and what it should say.

The other issue with "Full Faith and Credit" statutes is that some states have search warrant statutes that require a police officer to execute the search. The next section discusses the issue of police turning over responsibility for executing the search to non-police personnel.

3. *Putting the Search in the Hands of Non-Sworn, Non-Government Personnel and the Conflict with State Statutes*

Police are not executing ISP search warrants, in the traditional sense. Instead of physically searching or even physically serving the warrant on a person and supervising that person while they conduct the search, state and local police routinely fax the warrant to the ISP. Civilian personnel then locate the records and fax them to the requesting officer.

Many state statutes require that police officers execute search warrants.[23] The reasoning behind these statutes is to ensure that searches are properly conducted and that the search remains within the scope of the warrant.[24] Of course, it is practically impossible for police to execute a search of an ISP for information. At the very least, officers would have to ask ISP personnel to assist them. Also, ISPs are often outside the officer's jurisdiction. Traveling to the ISP to physically serve the warrant or conduct the search would be virtually impossible.

As stated earlier, the federal search warrant statute allows for agents to enlist the assistance of non-government personnel and has been interpreted not to require the presence of federal agents.[25] Each state has its own laws governing execution of searches and whether or

23. *Supra* n. 21.

24. *Morris v. State*, 622 So. 2d 67 (Fla. 4th Dist. App. 1993)

25. 28 U.S.C. § 3105; *U.S. v. Bach*, 310 F.3d 1063, 2002 U.S. App. LEXIS 23726 (8th Cir. 2002) cert. denied, 123 S. Ct. 1817, 155 L. Ed. 2d 693, 2003 U.S. LEXIS 3174, 71 U.S.L.W. 3667 (2003).

not civilians may assist. The states have yet to come face-to-face with these issues, but they no doubt will.

a. Two Cases that Demonstrate the State Search Warrant Problem: United States v. Bach and *Freedman v. America Online*

Two recent cases provide examples of how state and local police execute search warrants for ISP information. The first case discussed is *United States v. Bach,*[26] followed by *Freedman v. America Online.*[27]

In *United States v. Bach*, a Minnesota police officer in one state faxed a search warrant for the contents of Bach's Yahoo! e-mail account to the ISP in California. That action violated Minnesota's statute governing execution of search warrants.[28] The officer was a member of a multi-agency task force established to investigate online child exploitation.[29] When it came time to arrest Bach, a federal agency arrested him, not state or local authorities.[30]

When Bach moved to suppress evidence obtained by faxing the search warrant to Yahoo!, the District Court granted the motion.[31] On appeal, the Eighth Circuit Court of Appeals overturned the District Court decision and dodged the state search warrant issue.[32]

The Circuit Court held that faxing the search warrant violated the state law requiring police to execute the search, and the ECPA was violated. However, suppression of evidence is not an option for violation of the ECPA.[33] The court held that the federal search warrant statute does not codify the Fourth Amendment to the Constitution.[34] If it had, the court would have suppressed the evidence. In dicta, the court cited that Congress created a privacy interest in e-mail that under *Smith v. Maryland*[35] would probably otherwise not exist.[36] The court upheld the Ya-

26. *Bach*, 310 F.3d 1063.

27. 303 F. Supp. 2d 121; 2004 U.S. Dist. LEXIS 1722 (D. Conn. 2004).

28. *Bach*, 310 F.3d at 1065; The statute states:

> A search warrant may in all cases be served anywhere within the issuing judge's jurisdiction by any of the officers mentioned in its directions, but by no other person, except in aid of the officer on the officer's requiring it, the officer being present and acting in its execution. An officer serving and executing a warrant shall notify the chief of police of an organized full-time police department of the municipality or, if there is no such local chief of police, the sheriff or a deputy sheriff of the county in which service is to be made prior to service and execution.

Minn. Stat. § 626.13.

29. *Bach*, 310 F.3d at 1065.

30. *Id.*

31. *Id.* at 1066.

32. *Id.* at 1068.

33. Minn. Stat. § 626.13.

34. *Bach*, 310 F.3d at 1066-67.

35. *Smith*, 442 U.S. 735.

36. *Bach*, 310 F.3d at 1066.

hoo! search's reasonableness, citing a number of state court holdings that approve civilian searches for bank records, software and other similar matter.[37] This holding works only because Bach was prosecuted in federal court. If he had been prosecuted in a Minnesota court, the result likely would have been different.

The United States District of Connecticut recently decided a case with similar beginnings in *Freedman v. America Online*.[38] Freedman sued AOL, the Town of Fairfield and two of its police officers after they obtained subscriber information from AOL using an unsigned search warrant application that they faxed directly to the company.[39] The Fairfield Police got involved after two town council members received an e-mail saying "the end is near."[40] The town council members complained that the message was threatening.[41] Two Fairfield officers signed a search warrant application and faxed it to AOL requesting the e-mail sender's subscriber information.[42] AOL faxed the information back.[43] Freedman sued under, among other things, the ECPA.[44]

The District Court did not touch on whether or not the officers *needed* a search warrant for the plaintiff's subscriber information. Under the ECPA, all that would have been required would have been an administrative subpoena.[45] The District Court granted summary judgment to the plaintiff as to the police officers because it found that they violated the ECPA.[46] By merely attesting to the facts and faxing it to AOL, the court found that the officers violated the ECPA.[47] Unbelievably, federal authorities do the same thing when they issue administrative subpoenas

---

37. Civilian searches are sometimes more reasonable than searches by officers. *Harris v. State*, 401 S.E.2d 263, 266 (Ga. 1991) (stating that a dentist may execute a search warrant for dental X-rays and impressions); *Schalk v. State*, 767 S.W.2d 441, 454 (Tex. App. 1988) (providing that a search by a civilian software expert more reasonable than search by an officer because the officer lacked knowledge to differentiate a trade secret from a legitimate computer software program), cert. denied, 503 U.S. 1006 (1992); *State v. Kern*, 914 P.2d 114, 117-18 (Wash. Ct. App. 1996) (indicating that it is reasonable to delegate search of bank records to bank employees, even when police officer was not present during the search). Civilian searches outside the presence of police may also increase the amount of privacy retained by the individual during the search. See *Rodriques v. Furtado*, 575 N.E.2d 1124 (Mass. 1991) (body cavity search done outside presence of officers); *Commonwealth v. Sbordone*, 678 N.E.2d 1184, 1190, n. 11 (Mass. 1997). *Bach*, 310 F.3d at 1064.

38. *Freedman*, 303 F. Supp. 2d 121.

39. *Id.* at 123.

40. *Id.* at n. 4.

41. *Id.*

42. *Id.* at 123.

43. *Freedman*, 303 F. Supp. 2d at 123.

44. *Id.*; 18 U.S.C. § 2707 (2004).

45. 18 U.S.C. § 2703(c)(2)(2004).

46. *Freedman*, 303 F. Supp. 2d at 129.

47. *Id.*

for ISP subscriber information, but they have yet to be held liable for it. The District Court did not address whether or not the police officers' inherent authority authorized them to issue an administrative subpoena or not.

One could argue that the police executed the search warrant at the time the police officer faxed the warrant.[48] That is neither intellectually nor factually honest. A contract may be "executed" upon signing, but a search warrant is "executed" only when police actually conduct the search. The language of the ECPA refers to "obtaining" the warrant rather than "executing" it as the point where an ISP must disclose information. The ECPA states that

> [a] governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—(A) *obtains* a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant.[49]

Note that the statute explicitly refers to "obtaining" the search warrant, not "executing" the search warrant.

Although the language is plain, the argument is flawed. If ISPs had to produce information upon obtaining search warrants, the whole process of serving the warrant or executing it would be unnecessary. Police officers could obtain search warrants and by some sort of magic the ISP would know about the warrant and be obliged to produce the information. The ECPA is not clear about how state warrants should be executed (and, by the way, it isn't clear that Congress has the authority to tell states how to execute warrants.) Just because the statute does not state how police must execute the warrant does not mean that simply obtaining a warrant is sufficient.

Search warrants are executed when the search is executed. (Otherwise, why would it be called a "search warrant?") Arguing anything other than that is an attempt to make a square peg fit in a round hole. The purpose of mandating that police officers execute searches is to ensure that individuals with training and experience in the law of search and

48. *See State v. Kern*, 81 Wn. App. 308, 914 P.2d 114 (Wash. 1996) holding that a warrant issued for a search of the defendant's bank records was executed when served, that it was completed in a timely manner, that the defendant was not entitled to notice of the search, that delegation of the search to bank officials was not improper, and that any procedural error pertaining to the inventory of items seized involved a ministerial function that did not prejudice the defendant. *See also State v. Signore*, 2001 Conn. Super. LEXIS 3569 (2001) (arguing that 18 U.S.C. § 2703 plainly states that ISPs must provide information upon police "obtaining" a warrant).

49. 18 U.S.C. § 2703(c) (2003).

seizure, together with a sworn duty to uphold the law conduct the search. If the legislature thought it would be permissible to delegate search execution authority, it would explicitly say so. Some state courts have made exceptions in some cases to authorize searches conducted by civilians,[50] but that does not translate into fifty states going along for the ECPA ride.

D. Lack of State Resources

The ECPA and globalization of the economy may very well herald the end of strict interpretation and signal an even greater concentration of power in the federal government.[51] This shift of power would be due, chiefly, to the states' relative lack of resources. State and local law enforcement do not know the proper protocols for obtaining ISP-held information because they lack the training and resources to fully research the issue and to educate the appropriate personnel in what each state believes to be the proper procedure.

When the states lack resources to launch a new effort, they usually rely on the federal government for grant funding or for technical assistance. Unfortunately, in this area the federal government has not been very helpful.[52] Nor should they be. The issue of states and local authorities obtaining information from ISPs is a state issue. It should be resolved by the states, and the federal government cannot answer state questions in the matter. If it could, what powers have the states retained? Have they delegated all of their inherent responsibilities to the federal government?

Few resources exist for local and state authorities that instruct them in the proper legal process to use and to obtain the information they seek from Internet service providers ("ISPs") or other online digital evidence. At the local and state level, the hurdles to investigating online crime are daunting. Of course, the states lack the necessary expertise, budget and plan to train, equip, recruit and retain the personnel needed to carry out this task. So, the states usually look to the federal government for answers, which creates the never ending cycle in which state questions regarding obtaining information held by Internet service providers is never resolved.

---

50. *See supra* n. 38.

51. The enormous costs of corruption and complying with unfunded federal mandates weighs in heavily on this discussion, but is reserved for another round of rambling discourse.

52. For instance, guidance from the federal authorities includes that state court issued § 2703(d) orders are not valid outside of the issuing state, but that conclusion is not necessarily true. Computer Crimes and Intellectual Property Section, supra n. 19.

IV. HOLD ON JUST ONE MINUTE! WHO IS CONGRESS TO TELL THE STATES WHAT TO DO?

It has not been settled that the Congress has absolute authority to govern all aspects of the Internet. The ECPA assumes that Congress holds the authority to tell state law enforcement and courts how they may obtain information held by ISPs. Presumably, Congress relied on its authority to regulate interstate commerce when it enacted the ECPA.[53]

However, the Internet is a universe in which interstate commerce is but one aspect. When states seek information from ISPs, most likely the information is necessary for the investigation of a crime. The criminal law has traditionally been the ambit of the states, not the federal government. The states authority to investigate crimes over which they have jurisdiction is usurped by the ECPA's requirements.

Certainly, federal law preempts state law in areas over which the United States Constitution enumerates Congressional authority.[54] Regulating interstate commerce is an enumerated power.[55] Governing the jurisdiction of the states' law enforcement agencies and courts is not an enumerated power.

Congress cannot grant state courts greater authority than state statutes and court rules allow. At the same time, the United States Constitution Due Process Clause limits the extent of the states' jurisdictional reach. While the Constitution sets the boundaries within which states may reach, the Congress has a completely different and limited role with regard to state power.

> The several States of the Union are not, it is true, in every respect independent. . . But, except as restrained and limited by [the Constitution], they possess and exercise the authority of independent States, and the principles of public law . . . are applicable to them. One of these principles is, that every State possesses exclusive jurisdiction and sovereignty over persons and property within its territory.[56]

V. WHAT'S MY MOTIVATION? CIVIL REMEDIES FOR FAILURE TO COMPLY WITH THE ECPA—DOH!

The ECPA provides for a civil cause of action for violating its mandates. There have been several cases that have affirmed the cause of action against state and local violations of the ECPA. None, so far, have been addressed by the United States Supreme Court, and none have

53. U. S. Const. art. I, § 8.

54. Federal preemption in cases of enumerated powers dates back to *Gibbons v. Ogden*, 22 U.S. 1, 6 L. Ed. 23, 1824 U.S. LEXIS 370, 9 Wheat. (1824).

55. U. S. Const. art. I, § 8.

56. *Pennoyer v. Neff*, 95 U.S. 714 (1878).

dealt with the issue of federal authority to dictate legal process regarding information held by ISPs.

Freedman v. America Online is one recent example. The Connecticut District Court granted partial summary judgment to the plaintiff, holding that local police officers violated the ECPA by faxing an unsigned warrant to AOL to obtain subscriber information.[57]

The Connecticut District Court heavily relied on *McVeigh v. Cohen*,[58] which involved a Navy officer who contacted AOL and requested information about the identity of the plaintiff during the course of an administrative inquiry. The court noted that the Navy officer's actions were probably in violation of the ECPA.[59]

VI. SO, NOW WHAT? POSSIBLE SOLUTIONS TO THE STATE ECPA PROBLEM

At the turn of the twentieth century, technology both advanced to the point where circumstances demanded changes in the common law way of doing things and forced the fashioning of new legal tools. Advances in transportation gave rise, at the time, to motor vehicles that crossed into other states. It was inevitable that the cars would have accidents and cause injury to people and property. The long-arm statute was born of the consequences of the advances in technology that enabled increased mobility.[60]

At the turn of the twenty-first century the states face a similar situation that is even more complicated and far-reaching. The Internet brings greater mobility than the motor vehicle. Whereas the car enabled bank robbers to drive into a state, hold up a bank and race back across the border, the Internet presents a much greater challenge. Bank robbers do not have to leave the comfort of their bedrooms to hold up the bank in a neighboring state, or a jurisdiction on the opposite side of the world, for that matter. Using the Internet, cybercriminals can quickly enter and exit a jurisdiction, leaving behind few clues for police to trace. At the present time, the lack of legal tools to investigate cybercrime at the state and local level gives cybercriminals an optimal advantage. One hundred years ago, a horse was almost as fast as a car. The police caught up to the bank robbers eventually. Today, the speed of the Internet, the transience of digital evidence and the impediments facing state and local police in their fight to obtain information militate against law enforcement. Cybercriminals use law enforcement weaknesses to their advantage, exploiting vulnerabilities and making the Internet a veritable

57. *Freedman*, 303 F. Supp. 2d 121.
58. 983 F. Supp. 215 (D.D.C. 1998).
59. *Id.* at 219.
60. Scoles & Hay, *supra* n. 11, at § 8.32.

"wild, wild West." The need for new tools is exigent and clear. But, what types of tools and who should fashion them is not so clear. This section discusses proposals for new investigative tools.

The National Institute of Justice (NIJ) has developed a legislative proposal aimed at facilitating state legal process to obtain information held by Internet Service Providers. The proposed bill is as follows:

> Full Faith and Credit - Any production order issued that is consistent with subsection (b) of this section by the court of another State (the issuing State) shall be accorded full faith and credit by the court of another State (the enforcing State) and enforced as if it were the order of the enforcing state.
>
> Production Order - A production order issued by a State court is consistent with this subsection if -
>
> (1) The order is pursuant to the investigation or prosecution of a crime of the issuing state;
>
> (2) The order was issued in accordance with the law of the issuing state; and
>
> (3) Such court had jurisdiction over the criminal investigation or prosecution under the law of the issuing state.
>
> "Production Order" means any order, warrant, or subpoena for the production of records, issued by a court of competent jurisdiction. "Records" includes those items in whatever form created or stored.[61]

The limitation of the NIJ proposal is that it is not within the authority of Congress to mandate the states to afford full faith and credit to anything other than final judgments.[62] Although Congress has authority over the Internet by virtue of its Commerce Clause power,[63] it does not have authority over the subpoenas, court orders and search warrants issued by state courts. There may be an argument that states are obliged to honor these legal processes, but such a duty is moral, not constitutionally imposed.[64]

A. Uniform State Legislation: Hybrid Warrant/Orders

One approach might be development of model legislation to create a new type of legal process for states. The National Conference of Commissioners on Uniform State Laws might be persuaded to study the issue

61. Thanks to Robert M. Morgester, Deputy Attorney General, Special Crimes Unit, California Department of Justice for the reference.

62. "A judgment rendered in one State of the United States need not be recognized or enforced in a sister State if such recognition or enforcement is not required by the national policy of full faith and credit because it would involve an improper interference with important interests of the sister State." *Restatement (Second) of Conflict of Laws* § 103 (1988 Revisions).

63. U. S. Const. art. I, § 8.

64. *Strader v. Graham*, 51 U.S. 82, 13 L. Ed. 337, 1850 U.S. LEXIS 1454, 10 HOW 82 (1851).

and develop a proposed uniform law. At the present time, there is no committee with direct cognizance of the issue, but there is a "Computer-Generated Evidence" Committee that could serve as a resource.[65] State legislatures could create hybrid search warrants that operate like court orders mandating production of records. As previously mentioned, some state courts have made exceptions to the strict requirement that police must execute search warrants and have allowed civilians to do so. This exception is sensible, but it is in derogation of the plain language of many state statutes. What happens in reality is that police justify the need to obtain stored communication content by detailing probable cause to a judge who issues a search warrant. Instead of executing the search warrant, police fax or serve the warrant and the ISP does the searching. ISP personnel produce the records. State legislation is required if the state does not already authorize a search warrant to be executed outside the state by non-sworn, non-government personnel.

Such action is not without precedent. The Privacy Protection Act serves as an example. In order to obtain records held by newspapers and publishers pursuant to the Privacy Protection Act ("PPA") police must use a subpoena.[66] The reason Congress enacted the PPA was that police executed a search warrant at a California university, student newspaper in search of information that would assist in identifying suspects in an investigation.[67] The newspaper objected to the search, but the courts upheld it, finding that the police did exactly what they should have. Congress enacted the PPA to ensure that instead of conducting a search of publishers' files, police give the publisher the opportunity to produce them. This practice protects the privacy of individuals who are not the subject of the investigation.

B. Long-Arm Statutes

In order to ensure that state subpoenas, court orders and newly created hybrid search warrants are honored in other states, states would need to have long-arm statutes that give the issuing court jurisdiction. Long-arm language of existing statutes will require revisiting so that legal process for ISP records will be effective.

VII. CONCLUSION

This article addressed methods available to compel production of information from ISPs pursuant to the ECPA and the continuing confusing state and local law enforcement face. The fifty individual and sovereign

65. The National Conference of Commissioners on Uniform State Laws can be located online at http://www.nccusl.org.

66. 42 U.S.C. § 2000aa (2004).

67. *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978).

states bring a multitude of varying laws and practices that vary from the federal law in real and substantial ways. The ECPA brings these differences between federal and state laws to our attention. State limitations when investigating cybercrime needs to be addressed. This article discussed approaches to resolve the confusion and make obtaining ISP records easier for state and local law enforcement.