Chapter 2

ON THE LEGALITY OF ANALYZING TELEPHONE CALL RECORDS

C. Swenson, C. Adams, A. Whitledge and S. Shenoi

Abstract This paper examines the legal issues related to the access and use of call detail records (CDRs) of telephone subscribers that are maintained by service providers. The scenarios considered involve a federal law enforcement agency obtaining CDRs to identify suspects in a terrorism investigation; a federal, state or local law enforcement agency analyzing CDRs to gain insight into drug trafficking activities by an organized crime family; and a state or local law enforcement agency using CDRs to identify parole violators or motorists who exceed the posted speed limit. In addition, the legality of a service provider analyzing CDRs to support its direct marketing efforts is discussed.

Keywords: Call detail records, collection, analysis, legal issues

1. Introduction

Telephone conversations are sacrosanct in the United States. Aside from the caller and receiver, it is illegal for a private entity to eavesdrop on or record a conversation. Law enforcement authorities may intercept and record specific conversations, but only with a court order.

However, a wealth of other information about telephone conversations and other communications is routinely collected and preserved by telecommunications service providers. This non-content information includes who communicated with whom, from where, when, for how long, and the type of communication (phone call, text message or page). Other information that is collected may include the name of the subscriber's service provider, service plan, and the type of communications device (traditional telephone, cell phone, PDA or pager).

Typically, non-content information is collected in the form of call detail records (CDRs) that are generated by telephone switches mainly for

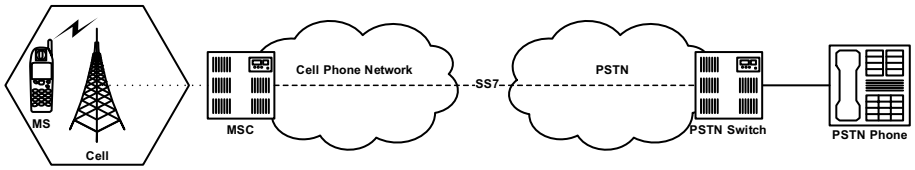

Figure 1. Telecommunications network schematic.

billing purposes [2, 4]. CDRs are created whenever a subscriber makes or receives a call, sends or receives a text message or page, or moves to a new area of coverage. CDRs also identify the cellular towers on which calls were placed and received. Since cellular towers only serve limited geographical regions and all hand-offs between towers are recorded, by analyzing information in CDRs, it is possible to pinpoint a mobile subscriber's location at a specific time and the subscriber's movement over time [10]. Furthermore, location information can be refined using other data maintained by service providers, e.g., directions (azimuths) of mobile subscribers from cellular tower antennae and the power levels of subscriber-to-tower communications.

Because CDRs contain detailed information about subscribers and their communications, including subscriber movements and communication patterns, they can be extremely useful in criminal investigations. But CDRs have other uses. Applying data mining algorithms to large quantities of CDRs could yield valuable intelligence to a government agency attempting to combat terrorism or to a telecommunications service provider hoping to attract new subscribers.

This paper focuses on the legal issues related to the access and use of CDRs of telephone subscribers in a variety of scenarios: terrorism and organized crime investigations as well as more mundane situations such as identifying parole violators or motorists who exceed the posted speed limit. In addition, the legality of service providers applying data mining algorithms on CDRs for use in direct marketing efforts is discussed.

2. Telecommunications Networks

This section describes the architecture of modern telecommunications networks and provides details about the collection, storage and format of CDRs.

2.1 Network Architecture

Figure 1 presents a schematic diagram of a modern telecommunications network. The core is the public switched telephone network

Table 1. Cellular protocols and providers.

Protocol	Providers
CDMA2000	Verizon, US Cellular
GSM	T-Mobile, Cingular/AT&T
Proprietary	Sprint, Nextel, Cricket

(PSTN), which is controlled by the Signaling System 7 (SS7) protocol [8]. The PSTN incorporates numerous switches that provide service to subscribers using land lines (i.e., traditional telephones).

Cellular networks interface with the PSTN using the SS7 protocol. A cellular network is divided into cells, each served by a cellular tower (base station). The towers enable mobile subscribers (MSs) to make calls. A mobile switching center (MSC) is the heart of a cellular network, permitting subscribers to move seamlessly from cell to cell with automatic reuse of resources.

Three main cellular network technologies are deployed in the United States (Table 1). The newer CDMA2000 networks evolved from (and are usually compatible with) the older CDMA/IS-95, TDMA and AMPS networks [6]. GSM, an international standard built on SS7, is growing in popularity; it will eventually be replaced with UMTS, a more advanced system [3]. Most of the proprietary protocols in use in the United States are based on CDMA2000 technology; they are incompatible with other systems and do not allow roaming with other providers.

2.2 Call Detail Records

Call detail records (CDRs) are logs containing data about communications, not the content of the communications [2]. They are generated during setup (initiation) and teardown (termination) of calls, faxes, SMS messages and pages as well as during certain kinds of hand-offs and roaming events, such as when a subscriber moves from one provider to another or from one region to another. Typically, they are generated by PSTN switches and by MSCs in cellular networks.

CDRs are generated primarily for billing purposes. However, service providers often use CDRs to detect instances of telecommunications fraud, and to support network management and traffic engineering.

The GSM 12.05 Standard specifies 19 different CDR types for GSM networks (Table 2) [4]. Other cellular networks record similar types of information.

Table 2. Standard CDR types (GSM networks).

1. Mobile Originated Call	11. VLR Update
2. Mobile Originated Emergency Call	12. HLR Update
3. Mobile Originated Forwarding	13. Mobile Originated SMS
4. Mobile Terminated Call	14. Mobile Terminated SMS
5. Roaming Call	15. SMS-MO Internetworking
6. Incoming Gateway Call	16. SMS-MT Gateway
7. Outgoing Gateway Call	17. Common Equipment Usage
8. Transit Call	18. Reduced Partial Records
9. Supplementary Services	19. CAMEL Interrogation
10. HLR Interrogation	

Table 3. GSM mobile-originated CDR fields.
(M = mandatory, C = conditional, O = optional)

Field	**Type**	**Description**
Record Type	M	Mobile originated
Served IMSI	M	IMSI of calling party
Served IMEI	C	IMEI of calling party (if available)
Served MSISDN	O	Primary MSISDN of calling party
Called Number	M	Number dialed by caller
Translated Number	O	Called number after MSC translation
Connected Number	O	Actual connected number (if different)
Recording Entity	M	Visited MSC producing the record
Location	M	Cell ID of originating call
Change of Location	O	Timestamped changes in location and cell ID
Event Timestamps	C	Incoming traffic channel assignment
	C	Answer
	O	Release
Call Duration	M	Duration of call or holding time
Cause for Termination	M	Reason for connection release
Diagnostics	O	More detailed reason for connection release
Sequence Number	C	Sequence number for partial records
Call Reference	M	Local identifier distinguishing MS transactions
Record Extensions	O	Network/manufacturer-specific extensions

The format of a CDR depends on the configuration of the switch that generates the record. Table 3 presents an example CDR for a GSM 12.05 mobile-originated call record. In GSM, the IMSI is a unique identifier for a subscriber, the IMEI is an identifier for a handset, and the MSISDN is a phone number.

CDRs typically require very little storage. Most events produce CDRs of at most a few hundred bytes. Even though billions of events occur daily, the total volume of CDRs collected and stored is manageable [7]. However, service providers may retain CDRs for limited (and variable) periods of time. In some cases, providers may archive only summarized information from CDRs.

The following sections discuss four scenarios related to the access and use of CDRs by law enforcement authorities and service providers.

3. Terrorism Investigation

Consider the following terrorism investigation scenario:

> *A reliable informant has indicated that J.S., a resident of Anytown, USA, has been calling individuals in North Waziristan, a tribal region straddling the Afghanistan-Pakistan border. May a U.S. law enforcement agency obtain from J.S.'s telephone service provider all available CDRs related to J.S.'s outgoing and incoming calls so it can identify and investigate members of J.S.'s calling groups?*

Records of telephone calls are treated differently than the contents of telephone conversations. The Supreme Court has ruled that the surreptitious eavesdropping and recording of private conversations constitutes a search under the Fourth Amendment, because there is a reasonable expectation of privacy in the contents of telephone calls [27, 28]. In contrast, the Court has decided that there is no expectation of privacy in information disclosed to a third party [26, 29]. CDRs are analogous to the address information on an envelope, which is used to direct correspondence to its location. Just as there is no reasonable expectation of privacy for address information, there is no reasonable expectation of privacy for CDRs and other customer proprietary network information (CPNI), which belong to the service provider rather than the subscriber.

In Smith v. Maryland [30], the Supreme Court decided that the government's use of a pen register to record the numbers dialed from a suspect's telephone differed significantly from the electronic eavesdropping and recording of telephone calls, because the pen register did not acquire the contents of telephone conversations. Without obtaining either a warrant or a court order, law enforcement agents in the Smith case asked a telephone company to install a pen register at the company's central offices to record the numbers dialed from a telephone at the defendant's home. After the pen register showed a call to a robbery victim, the police obtained a search warrant for the defendant's home. The Supreme Court decided that the defendant had no legitimate expectation of privacy regarding the telephone number that he had called, because when he used his telephone, he voluntarily conveyed the number

to the phone company for use in the ordinary course of business. The Court pointed out that subscribers realize that a phone company has facilities for making permanent records of the numbers they call, because their telephone bills include a list of the toll calls they made. The Court also ruled that the defendant assumed the risk that the phone company would disclose the telephone numbers to the government, even though the company used automatic switching equipment instead of a live operator to place the calls. The Court concluded that "[t]he installation and use of a pen register ... was not a search, and no warrant was required."

The Smith decision dealt only with pen registers, which record the telephone numbers for outgoing calls; it did not address trap and trace devices that record the telephone numbers for incoming calls, or the CDRs that are created by service providers. Trap and trace devices and CDRs differ from pen registers in that subscribers may not be aware that a phone company can keep track of incoming calls like it records information about outgoing toll calls for billing purposes. On the other hand, trap and trace devices and CDRs are similar because they do not provide access to the contents of the communications. Therefore, under the Smith decision, installing a trap and trace device or obtaining a suspect's CDRs would not constitute a "search" under the Fourth Amendment. Accordingly, the Fourth Amendment would not require a law enforcement agency to obtain a warrant to install a trap and trace device or to obtain CDRs from a service provider.

While the Fourth Amendment does not require a warrant for obtaining CDRs, law enforcement agencies must satisfy statutory requirements to do so. The particular statutory requirements depend on which of the following three categories of information is sought by law enforcement: (i) contents of electronic communications, (ii) stored records, and (iii) real-time information other than the contents of electronic communications. The contents of telephone communications are governed by the Wiretap Act of 1968, which not only makes electronic eavesdropping and wiretapping crimes punishable by up to five years imprisonment ([19] § 2511(4)), but also prescribes the procedure that law enforcement agencies must follow to obtain authorization for electronic eavesdropping and wiretapping ([19, 23] § 2516). The Electronic Communications Privacy Act (ECPA) of 1986 extended the Wiretap Act to cover the interception of electronic communications in addition to oral and wire communications, which the Wiretap Act had previously covered. The ECPA also added the Stored Communication Act ([19, 23] §§ 2701–2711), which covers stored records and prohibits access to stored electronic communications unless authorized by a court order. Lastly, the ECPA added the Pen Register and Trap and Trace Device Statute ([19, 23] §§ 3121–3127),

which covers real-time information other than the contents of electronic communications and prohibits the use of pen registers and trap and trace devices, unless authorized by a court order.

Section 2511 of Title 18 of the United States Code [19] prohibits the unauthorized interception of wire, oral or electronic communications. "Intercept" is defined broadly as the acquisition of the contents of any wire, oral or communication through the use of any device ([19] § 2510(4)). Law enforcement personnel may obtain authorization for the interception of electronic communications by obtaining a court order under Section 2518, but the statute requires a showing of probable cause that the subject of the order is committing, has committed, or is about to commit a crime. Section 2511 would not apply to the scenario under consideration because it is only J.S.'s CDRs, as opposed to the contents of J.S.'s communications, that are being sought.

The means required for a law enforcement agency to obtain J.S.'s CDRs depend on the type of information that the agency is seeking. For land line telephones, the CDRs sought by an agency may include the date, time and duration of each call, the number called and the charges. Since each land line telephone is associated with a specific address, the telephone numbers can identify the physical locations of the calling and called parties. Similar information may be obtained for mobile networks, including the dates, times and durations of calls, and the originating and dialed numbers. In addition, information about the caller's approximate physical location may be revealed by CDRs.

Section 2703(c)(2) of Title 18 [23] requires a service provider to supply the following types of customer information in response to a grand jury subpoena: the customer's name and address, local and long distance connection records, records of session times and durations, telephone or instrument number, and the means and sources of payment for the service. The showing required for issuance of a grand jury subpoena is that the information sought may be relevant to the purpose of the grand jury investigation.

Instead of using a grand jury subpoena, a law enforcement agency may obtain J.S.'s past CDRs by complying with the requirements of the Stored Communications Act, which governs stored records. Section 2703 of Title 18 [23] prohibits a service provider from disclosing subscriber records to any government entity without the subscriber's consent unless the government entity obtains either a warrant or court order for the disclosure. A court order for the disclosure may issue only if the government entity offers specific and articulable facts showing that there are reasonable grounds to believe that the CDRs sought are relevant to an ongoing criminal investigation ([23] § 2703(d)). Penalties

for a violation include actual damages of no less than $1,000, punitive damages and reasonable attorney fees ([19] § 2707(c)). In addition, the government entity may be subject to disciplinary action for a willful violation ([23] § 2707(d)).

If the law enforcement agency is seeking prospective CDRs, it would need to satisfy the Pen Register and Trap and Trace Device Statute, which governs real-time information other than the contents of electronic communications. Section 3121(a) of Title 18 [19] provides: "Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under Section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (Title 50 U.S.C. 1801 *et seq.*)." The terms "pen register" and "trap and trace device" are defined broadly in Section 3127 [23] (as well as in the Foreign Intelligence Surveillance Act (FISA)) to cover CDRs. Section 3122 [19] authorizes federal, state and local law enforcement officers to apply for an order for the installation and use of a pen register or trap and trace device. Section 3123 requires the court to issue the order if it finds that a "law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." Thus, in our scenario, law enforcement personnel would be able to obtain J.S.'s CDRs if they can certify to a court that they are relevant to a current criminal investigation.

Alternatively, past CDRs may be obtained under Section 2709 of Title 18 [19, 23] and prospective CDRs may be obtained under FISA if they are relevant to an investigation to protect against international terrorism or clandestine intelligence activities. Section 2709 imposes a duty on a service provider to provide a customer's name, address, length of service, and local and long distance billing records upon the request of a designee of the FBI Director, who certifies in writing that the information is relevant to an investigation to protect against international terrorism or clandestine intelligence activities. This certification is known as a National Security Letter (NSL). In contrast to other means for obtaining CDRs, no court order is required for an NSL.

In addition, Section 1842 of Title 50 of the United States Code [21] provides that designated attorneys for the United States may apply for an order from the FISA court for the installation and use of a pen register or trap and trace device to obtain prospective CDRs. The application must include a certification that the information likely to be obtained is foreign intelligence not concerning a U.S. person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that the investigation of the U.S.

person is not conducted solely upon the basis of activities protected by the First Amendment ([21] § 1842(c)(2)). Therefore, in the scenario under consideration, the law enforcement agency could obtain the CDRs for J.S.'s calls by obtaining an order from the FISA court based on a certification that the CDRs are relevant to an ongoing terrorism investigation.

The requirements for a grand jury subpoena and the certification requirements under the Stored Communications Act, Pen Register and Trap and Trace Device Statute and FISA are significantly less stringent than the probable cause showing required for the issuance of a warrant. A showing of probable cause involves the demonstration of a fair probability that evidence of a crime will be found, and the determination of probable cause has to be made by a neutral judge or magistrate. In contrast, the certification requirements only involve relevance to an ongoing investigation, and the certification is made by law enforcement personnel or an attorney for the United States, rather than a neutral judge or magistrate. Even so, additional information besides the report that J.S. was calling North Waziristan would be required before a certification could be made that the CDRs are related to an ongoing terrorism or criminal investigation.

Once the CDRs are properly obtained, law enforcement officials would be free to investigate the communities of interest and the calling patterns they revealed as long as they do not access the contents of communications. Section 3121(c) of Title 18 [23] requires the government to use technology that restricts the information recorded by a pen register or trap and trace device so as not to include the contents of any wire or electronic communication. This is not an issue as CDRs do not contain any information about the contents of phone calls.

We now discuss a related, but somewhat broader, scenario involving the acquisition of CDRs:

> *U.S. intelligence sources in Pakistan indicate that members of a suspected terrorist cell in Anytown, USA have been communicating surreptitiously with individuals in North Waziristan. May a U.S. law enforcement agency obtain from the telephone companies serving Anytown, USA the CDRs of their subscribers so it can identify and investigate individuals who have made telephone calls to North Waziristan?*

This scenario differs from the previous one in that it involves obtaining the CDRs of all the subscribers in Anytown, USA, rather than just the CDRs for a single individual. As in the previous scenario, a U.S. law enforcement agency could access the CDRs by obtaining a court order based on a certification that the CDRs are related to an ongoing criminal or terrorism investigation. However, while the scope of an investigation

would probably extend to all the members of the suspected terrorist cell in Anytown, USA, it is difficult to see why it should extend to subscribers who are not members of the cell. Accordingly, it would be difficult to convince a court of the reasons for obtaining CDRs for all the subscribers in Anytown, USA.

This scenario addresses some of the allegations that have been made in several class action suits that have recently been filed against telecommunications companies for allegedly divulging customer records to the U.S. Government [1, 5]. A class action suit filed in San Francisco, which has been consolidated with seventeen other class actions, alleges that AT&T violated Section 2702(A)(3) of Title 18 of the Stored Communications Act by divulging customer records to the government [13]. The trial judge denied the U.S. Government's motion to dismiss the case on the grounds of the state secrets privilege. However, he stated that he might grant summary judgment later in the case, if he decided that the state secrets privilege would block essential evidence in the case. The judge also emphasized that he was not ruling on whether or not any of the allegations in the case were true [14].

4. Organized Crime Investigation

Consider the following scenario:

> *Law enforcement authorities investigating drug trafficking by an organized crime family intend to apply data mining algorithms on CDRs to identify the key players and collaborators, gain insights into command and control techniques, and glean information about drug shipment, distribution and sales patterns. May a law enforcement agency obtain from service providers the CDRs corresponding to phone calls made and received by several members of an organized crime family over a period of one year?*

As discussed in Section 3, a law enforcement agency would not require a warrant to obtain CDRs from a service provider. The Fourth Amendment originally applied only to federal government agencies, but the Supreme Court decided in a series of landmark cases in the 1960s that the Fourth, Fifth, Sixth and Eighth Amendments had been incorporated into the Fourteenth Amendment's guarantee of due process of law, which is applicable to state and local governments. Thus, the Fourth Amendment standards for unreasonable searches and seizures apply to federal, state and local law enforcement agencies [24, 25].

Similarly, the Wiretap Act, the Stored Communications Act, and the Pen Register and Trap and Trace Device Statute are all applicable to federal, state and local law enforcement agencies. Therefore, the agency would need to apply for an order to obtain the CDRs based on a cer-

tification that the CDRs are relevant to an investigation. As long as the CDRs are relevant to the investigation, they could be obtained for calls made and received by members of the organized crime family for a period of one year, or even longer. Federal law enforcement authorities would submit their applications to an appropriate federal court, while state and local agencies would submit their applications to an appropriate state or local court ([23] § 3127(2)).

Once the law enforcement agency obtains the CDRs, it may employ data mining algorithms to discover correlations and patterns. These could include identifying the key players and collaborators, obtaining insights into command and control techniques, and gleaning information about drug shipment, distribution and sales patterns.

It might be argued that the use of data mining algorithms to analyze CDRs constitutes an unreasonable search because it indirectly reveals information about the contents of calls made or received by the subjects. This argument might, for example, be based on Kyllo v. United States [33], where the Supreme Court decided that the government's warrantless use of a thermal imaging device directed at the inside of a private home to detect heat lamps for growing marijuana constituted an unlawful search. In reaching its decision, the Court emphasized that the thermal imaging device violated the occupant's reasonable expectation of privacy, because it involved the use of sensor technology that was not in general public use.

Similarly, it might be argued that the application of advanced data mining algorithms to the analysis of CDRs would constitute an unlawful search, because data mining algorithms are not in general public use and the public is not generally aware of data mining algorithms. On the other hand, data mining algorithms merely involve the discovery of correlations between seemingly unrelated events and then drawing inferences based on the correlations. Members of the general public should be quite familiar with the notion of detecting patterns in everyday life and, therefore, it should come as no surprise to them that law enforcement authorities would be able to detect useful patterns by analyzing CDRs.

5. Location-Time Information

Location-time information obtained from CDRs can be used to prove that individuals may be violating certain laws. Since cell towers can only provide service within a small geographical area, it is possible for investigators to use data from CDRs to estimate the whereabouts of subscribers at certain times. The following questions arise:

May a state or local law enforcement agency obtain from service providers the CDRs for convicted felons residing in its jurisdiction to determine whether they have violated certain terms of their parole (e.g., leaving the city, county or state)?
May a state or local law enforcement agency obtain from service providers the CDRs for all calls made and received in the vicinity of a turnpike to identify motorists who have exceeded the posted speed limit?

It appears that a law enforcement agency may be able to obtain historical information about the location of a particular cellular phone upon providing specific and articulable facts that the location is relevant and material to an ongoing criminal investigation. However, it would probably be necessary for law enforcement to obtain a warrant based upon a showing of probable cause to acquire prospective real-time information concerning the location of a cellular phone.

The U.S. Supreme Court considered the application of the Fourth Amendment to the monitoring of electronic tracking devices (beepers) in United States v. Knotts [31] and United States v. Karo [32]. In the Knotts case, the Court decided that law enforcement authorities did not require a warrant to monitor a beeper that was placed in a container of chemicals because the monitoring revealed no more than the authorities would have been able to observe through visual surveillance. In contrast, the Court decided in the Karo case that law enforcement authorities did require a warrant to monitor a beeper that was inside a private residence and not open to visual surveillance. The monitoring in Karo represented a greater threat to privacy because it involved an intrusion into a residence, while the monitoring in Knotts involved a suspect who was traveling in an automobile on public roads where the suspect had no reasonable expectation of privacy.

Under the Knotts and Karo cases, therefore, law enforcement authorities would not require a warrant to track the location of a cellular phone unless the phone was located in a private residence. Nevertheless, a number of U.S. magistrates have decided that a warrant is required for law enforcement authorities to obtain cell site information on account of the Communications Assistance for Law Enforcement Act of 1994 (CALEA).

CALEA was enacted to enable law enforcement agencies to retain their surveillance capabilities despite technological advances in the field of telecommunications. To accomplish this objective, CALEA requires service providers to ensure that their equipment will enable the government to intercept wire and electronic communications and access call-identifying information pursuant to lawful orders ([20] § 1002(a)(2)). During CALEA's Congressional hearings, the proposal was challenged on the grounds that it would authorize the tracking of cellular phone

users. However, the then FBI Director Freeh responded to these concerns by proposing the addition of language to the statute that would prevent the use of pen registers and trap and trace devices to track subscribers. Consequently, the following language was added at the end of CALEA's provision dealing with the requirement for telecommunications carriers to provide governmental access to call-identifying information:

> "[E]xcept that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices ([19] § 3127), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)" ([20] § 1002(a)(2)).

As a result of this provision, law enforcement authorities are barred from acquiring call-identifying information that would disclose the physical location of a subscriber "solely pursuant to the authority for pen registers and trap and trace devices." Nevertheless, government attorneys have sought to get around this provision and acquire cell site information without a warrant by seeking authorization under the Stored Communications Act. This act authorizes the government to obtain a court order for the disclosure of telephone records if it provides "specific and articulable facts" showing that the records are relevant and material to an ongoing criminal investigation ([23] § 2703(c),(d)). The standard for obtaining an order under the Stored Communications Act is similar to the standard under the Pen Register and Trap and Trace Device Statute, and it is less stringent than the standard for obtaining a warrant, which requires probable cause.

Several courts have accepted the government's argument and have granted orders authorizing the government to obtain cell site information [15, 17, 18]. However, the majority of courts have rejected the government's argument primarily because the Stored Communications Act was enacted to allow government access to records in storage, rather than as a means to conduct real-time surveillance through a prospective order for the disclosure of cell site information [11, 12, 16]. For real-time surveillance, the government must rely on the Pen Register and Trap and Trace Device Statute to obtain telephone records or on warrants if it wants to intercept communications or obtain other information. On the other hand, the government may acquire historical CDRs using the Stored Communications Act, and it appears that these could potentially include cell site information [11]. Service providers usually retain CDRs for limited periods of time, and so it is likely that these records might not be available by the time an order for their disclosure can be obtained.

The first question in the scenario is whether a law enforcement agency may obtain cell site information from CDRs for convicted felons to verify whether they have left the area they have been restricted to by the terms of their parole. As a practical matter, the granting of parole would normally be conditioned on consent to track the parolee's location and to the parolee's wearing a tracking device. Naturally, if the parolee's consent had been obtained, no court order would be needed for tracking the parolee. Thus, the remaining discussion presumes the lack of consent.

The majority of courts that have addressed the issue stipulate that the agency must obtain a warrant based on a showing of probable cause to acquire prospective cell site information. To obtain a warrant, the agency would need to show there is a fair probability that evidence of a crime would be found. A showing that an individual is a convicted felon would not be sufficient for issuance of a warrant, because it would not provide any basis for concluding that the person had violated a condition of parole. In addition, even if there were to be a showing that the individual had violated a condition of parole, it would not be sufficient for issuance of a warrant, because a parole violation is not a crime.

The courts that have issued orders for prospective cell site information have required a showing under the Stored Communications Act of specific and articulable facts that the information is relevant to an ongoing criminal investigation. This standard would not be satisfied because parole violations are generally not the subject of ongoing criminal investigations. If the agency sought historical cell site information from a service provider, it would need to rely on the Stored Communications Act, and this would require the same showing of specific and articulable facts that the information was relevant to an ongoing criminal investigation. Consequently, a law enforcement agency could not obtain cell site information from CDRs for convicted felons to check if they have violated conditions of their parole.

The second question is whether a law enforcement agency may obtain cell site information from CDRs for motorists driving on a turnpike to identify speeders. In contrast to a parole violation, speeding is a crime. Nevertheless, to obtain prospective cell site information, the agency would probably need a warrant, and this would require some showing that certain subscribers would be likely to be speeding on the turnpike. It is difficult to imagine how a convincing showing of this sort could be made. Therefore, the agency would not be able to obtain cell site information from CDRs to catch speeders.

6. Direct Marketing Efforts

"Roamers" are cellular subscribers who have signed up for service with one provider but use the network resources of another provider, for example, when they travel outside their service region. We consider the following question regarding the use of roamers' CDRs for direct marketing efforts by a service provider:

> *Since service providers own their CDRs, may a service provider analyze CDRs in its possession to identify roamers and their calling patterns and target them with customized service plans as part of its direct marketing efforts?*

This scenario differs from the previous scenarios because it involves a private entity rather than a government agency. Section 222 of Title 47 of the United States Code [20] applies across the board to government and private entities, and it would prohibit a service provider's use of CDRs for its own direct marketing efforts. Section 222(c)(1) provides:

> "Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories."

"Customer proprietary network information" (CPNI) is defined to include "information that relates to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service" ([20] § 222(h)(1)). Therefore, this information would include the identities of roamers and their calling patterns. Each violation is punishable by a fine of not more than $10,000 or imprisonment for a term not exceeding one year, or both ([20] § 501).

However, Section 222 specifies that CPNI may be used or disclosed with the approval of the customer. The regulations authorize service providers to obtain approval for the use or disclosure of CPNI from a customer either expressly or by failure of the customer to object within 30 days after receiving appropriate notification either in writing or by e-mail [22].

The use of CDRs may also be prohibited by state laws. For example, the State of Oklahoma prohibits the procurement of a telephone subscriber's records without the subscriber's authorization [9]. This prohibition is subject to a number of exceptions, including that a telecommunications company may obtain access to telephone records to provide service, to protect its rights, or to protect other subscribers or carriers

from unlawful uses of telephone service. The exception would not apply to the use of CDRs for a telecommunications company's direct marketing campaign.

7. Conclusions

CDRs have been traditionally used by service providers for billing purposes, network management, traffic engineering and fraud detection. Because they contain detailed information about subscribers and their communications, including subscriber movements and communication patterns, CDRs are very useful in law enforcement investigations and for gathering intelligence. In particular, the application of data mining algorithms to large quantities of CDRs may yield valuable intelligence to government agencies attempting to combat terrorism or crime, or to a telecommunications service provider hoping to attract new subscribers. However, several legal restrictions are in place to protect the privacy of innocent subscribers. Significant restrictions on the access and use of CDRs by government agencies are imposed by the Pen Register Trap and Trace Device Statute, the Communications Assistance for Law Enforcement Act (CALEA) and the Stored Communications Act. Telephone subscribers are also protected from wanton data mining by service providers by Title 47 of the United States Code and by various state laws. In general, law enforcement agencies may not access and use CDRs without a warrant or court order, which require a showing that the CDRs in question are relevant and material to a criminal or terrorism investigation. Furthermore, service providers may not use CDRs for non-business purposes without obtaining explicit authorizations from their subscribers.

References

[1] L. Cauley, NSA has massive database of Americans' phone calls, *USA Today* (www.usatoday.com/news/washington/2006-05-10-nsa_x.htm), May 11, 2006.

[2] Cisco, Call detail records (www.cisco.com/univercd/cc/td/doc/product/wanbu/das/das_1_4/das14/das14apd.htm).

[3] J. Eberspächer, H. Vögel and C. Bettstetter, *GSM: Switching, Services and Protocols*, Wiley, Chichester, United Kingdom, 2001.

[4] European Telecommunications Standards Institute, ETSI TS 100 616 V7.0.1 (1999-07), Digital Cellular Telecommunications System (Phase 2+), Event and Call Data (GSM 12.05 Version 7.0.1 Release 1998), 1998.

[5] G. Gross, NSA wiretap lawsuits transferred to California court, IDG News Service (www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9002385), August 11, 2006.

[6] S. Low and R. Schneider, *CDMA Internetworking: Deploying the Open A-Interface*, Prentice Hall, New Jersey, 2000.

[7] T. Moore, A. Meehan, G. Manes and S. Shenoi, Forensic analysis of telecom networks, in *Advances in Digital Forensics*, M. Pollitt and S. Shenoi (Eds.), Springer, New York, pp. 177–188, 2005.

[8] T. Russell, *Signaling System #7*, McGraw-Hill, New York, 2002.

[9] State of Oklahoma, Unauthorized or Fraudulent Procurement, Sale or Receipt of Telephone Records, Title 21, Section 1742.2, *2006 Supplement Oklahoma Statutes (Volume 1)*, Oklahoma City, Oklahoma, p. 1107, 2006.

[10] C. Swenson, T. Moore and S. Shenoi, GSM cell site forensics, in *Advances in Digital Forensics II*, M. Olivier and S. Shenoi (Eds.), Springer, New York, pp. 259–272, 2006.

[11] U.S. District Court (District of Maryland), In the matter of the application of the United States of America for an order authorizing the installation and use of a pen register and caller identification system on telephone numbers and the production of real time cell site information, *Federal Supplement Second Series*, vol. 402, pp. 597–605, 2005.

[12] U.S. District Court (Eastern District of New York), In the matter of the application of the United States of America for an order (i) authorizing the installation and use of a pen register and trap and trace device, and (ii) authorizing release of subscriber information and/or cell site information, *Federal Supplement Second Series*, vol. 396, pp. 294–327, 2005.

[13] U.S. District Court (Northern District of California), Hepting v. AT&T, Amended complaint for damages, declaratory and injunctive relief, No. C-06-0672-JCS, paragraphs 126–132 (www.eff.org/legal/cases/att/att_complaint_amended.pdf), 2006.

[14] U.S. District Court (Northern District of California), Hepting v. AT&T, Order, No. C-06-672-VRW, pp. 35–36 (www.eff.org/legal/cases/att/308_order_on_mtns_to_dismiss.pdf), 2006.

[15] U.S. District Court (Southern District of New York), In re application of the United States of America for an order for disclosure of telecommunications records and authorizing the use of a pen register and trap and trace device, *Federal Supplement Second Series*, vol. 405, pp. 435–450, 2005.

[16] U.S. District Court (Southern District of Texas), In the matter of the application of the United States for an order: (i) authorizing the installation and use of a pen register and trap and trace device, and (ii) authorizing release of subscriber and other information, *Federal Supplement Second Series*, vol. 441, pp. 816–837, 2006.

[17] U.S. District Court (Southern District of Texas), In the matter of the application of the United States for an order: (i) authorizing the installation and use of a pen register and trap and trace device, and (ii) authorizing release of subscriber and other information, *Federal Supplement Second Series*, vol. 433, pp. 804–806, 2006.

[18] U.S. District Court (Western District of Louisiana), In the matter of the application of the United States for an order: (i) authorizing the installation and use of a pen register and trap and trace device, and (ii) authorizing release of subscriber information and/or cell site information, *Federal Supplement Second Series*, vol. 411, pp. 678–683, 2006.

[19] U.S. Government, Title 18: Crimes and Criminal Procedures, *United States Code (Volume 9)*, Washington, DC, pp. 787–1675, 2001.

[20] U.S. Government, Title 47: Telegraphs, Telephones and Radio-Telegraphs, *United States Code (Volume 27)*, Washington, DC, pp. 1–317, 2001.

[21] U.S. Government, Title 50: War and National Defense, *United States Code (Volume 29)*, Washington, DC, pp. 1–724, 2001.

[22] U.S. Government, Customer Proprietary Network Information, Sections 64.2007–2009, Federal Communications Commission, *Title 47, Code of Federal Regulations*, Washington, DC, pp. 323-326, 2006.

[23] U.S. Government, Title 18: Crimes and Criminal Procedures, *United States Code Annotated Supplement*, Washington, DC, pp. 5–146, 2007.

[24] U.S. Supreme Court, Mapp v. Ohio, *United States Reports*, vol. 367, pp. 643–686, 1961.

[25] U.S. Supreme Court, Ker v. State of California, *United States Reports*, vol. 374, pp. 23–64, 1963.

[26] U.S. Supreme Court, Hoffa v. United States, *United States Reports*, vol. 385, pp. 293–322, 1966.

[27] U.S. Supreme Court, Berger v. United States, *United States Reports*, vol. 388, pp. 41–129, 1967.

[28] U.S. Supreme Court, Katz v. United States, *United States Reports*, vol. 389, pp. 347–374, 1967.

[29] U.S. Supreme Court, United States v. Miller, *United States Reports*, vol. 425, pp. 435–456, 1976.

[30] U.S. Supreme Court, Smith v. Maryland, *United States Reports*, vol. 442, pp. 735–752, 1979.

[31] U.S. Supreme Court, United States v. Knotts, *United States Reports*, vol. 460, pp. 276–288, 1983.

[32] U.S. Supreme Court, United States v. Karo, *United States Reports*, vol. 468, pp. 705–736, 1984.

[33] U.S. Supreme Court, Kyllo v. United States, *United States Reports*, vol. 533, pp. 27–52, 2001.