NTI | **Law Enforcement Systems and Services**

PO Box 99, Jefferson, NH 03583 (603) 586-7156 [fax… (603) 586-7164]

Enhancing Counter-Terrorism and Criminal Investigations with Telephonic Information

The need: Investigators are expected to assimilate and exploit many different forms of telephonic information. Telephone technology is constantly changing; new telephone services are added and, to support these services, additional data is stored in telephone company databases. That information is available to law enforcement under due legal process, but it is necessary that analysts are aware of how to obtain and use this data to maximize its potential. In addition, terrorists and criminals are constantly upgrading their "creative" use of the latest telephone technology to facilitate their operations and hide their contacts from law enforcement.

NTI's Training Services: Did you, personally, ever plan to do anything important to you without making at least one directly related telephone call to a person or business? Don't you think that any bad guy would be likely to make least one directly related telephone call to a person or business before, during, and/or after performing a criminal act, particularly if involved in a conspiracy to commit that act? If you can answer yes to these two rhetorical questions, you've justified the need for an in-depth look at telephone information in your investigations. Landline and cell telephones are probably the most common form of communication employed by criminals – even more so that face-to-face conversation! Yet, try to find a criminal justice college course or a law enforcement police academy or in-service training class on how to use telephone information to support investigations.

NTI's seminars are designed for working investigators at all levels to provide an in-depth introduction to strategies and techniques to identify and exploit criminal use of telephonic communication. In addition, special topics are covered in depth, such as how to proactively employ prepaid calling cards, "throw-away" cell phones, toll-free hot lines, and other techniques to support UC operations.

In providing direct support to law enforcement agencies on a number of different investigations, we have experience working with all types of telephonic communication records and stay current with the latest telephone technology. Specifically, NTI has provided telephonic analytical and/or investigative services supporting ongoing cases for the FBI, Diplomatic Security Services, ICE, 911 centers, New York Police Department, and other federal, state, and municipal law enforcement agencies, all within the last twelve months. During the course of those investigations, we have encountered a wide variety of situations, some of which required extensive research of the latest telephone technology to develop analytical and investigative methodologies. NTI has incorporated these new concepts into its already advanced telephonic training programs to offer what we consider to be the most up-to-date and comprehensive telephonic analytical and investigative training available. This training is available to federal agencies under GSA schedule contract **GS02F0004R** and is also offered in a version customized specifically for state and local Law Enforcement. You can access NTI's GSA schedule via the following link…

http://www.gsaelibrary.gsa.gov/ElibMain/ContractorInfo?contractNumber=GS-02F-0004R&contractorName=NORTHERN+TECHNOLOGY+INC&executeQuery=YES

Seminar Descriptions: Telephone Concepts for Support of Criminal and National Security Investigations

The following seminar descriptions are for individual classes covering the course material described; however, the material covered and detail to which it is covered can be customized to fit the schedule and needs of attendees. There are three options for class presentation…

1. Structured classes conforming to the specific descriptions below at an agreed-upon level of detail and instruction time
2. Custom classes where material is assembled from the class topics detailed below and targeted for a specific group of trainees and/or for a specific case or type of case.
3. Ad hoc hands-on training where the topics covered are case specific to a current agency investigation using actual case information. The focus of the class would be to generate leads and or evidentiary conclusions for the case.

Introduction

It's easy to regard subpoenaed toll and court-ordered pen register information as simplistic in concept, both providing the "basic five" call detail elements (date, time, duration, originating number, and destination number). After all, investigators and analysts are the ones who actually work with the data - the sorting, correlating, and analyzing of that information to produce links and chronologies that generate leads for the case. But control of the information presented to them for analysis is typically in the hands of the lead investigator and the prosecuting attorney. With the new technology, there can be a lot more call elements available than the "basic five". There is also a wealth of [usually untapped] information available from a subscriber subpoena. The telephone company won't give it to you unless you ask, and to "ask", you need a basic understanding of the latest telephone technology and services as well as how telephone company accounts are administered.

This seminar addresses the following areas:

1. What an investigator needs to know about landline and cell systems
2. What information is available from subscriber and call detail record (tolls) subpoenas
3. Applying for a court order even if you have no intent of implementing electronic surveillance
4. What information is available from court-ordered pen registers
5. What can we get from pay phones, PBX/CENTREX systems, prepaid cards, "throw-away" cell phones, satellite phones, etc.
6. Understanding telephone services and the information they can provide
7. Understanding the critical information available in telephone service account information
8. Managing the telephonic aspect of your investigation.

"Throw-away" Cell Phones

Well, you really don't have to throw the phone away – but you might if you're a bad guy and you want the ultimate in anonymity. This new service causes all kinds of headaches, but it's a bad news-good news situation. The bad news is that the bad guys can get a completely anonymous cell phone at a Wal-Mart for about $50. The good news is that he thinks the phone is untraceable

(but it is). Some “telephone-shy” individuals feel totally safe using the “throw-aways”. And that’s where we can get them. All the caution they may exercise when using landline or standard cell phones is thrown to the wind on a “throw-away”. It’s not as easy as a standard, subscribed-to cell phone, but using the techniques presented in this class will enable you to track down and get information about the subscriber, his call detail records (tolls) and even a Title III wire.

Criminal use of Telephone Technology to Avoid Detection and Prosecution

The fact that telephone call analysis has been used successfully in many investigations is well documented. Not only is this well known to law enforcement investigators and analysts, it is also known by criminals. Telephone calls are the "footprints" they leave when they contact their co-conspirators. They are as sensitive about these electronic footprints as a burglar would be about leaving his tracks in the mud as he is leaving a crime scene.

Just as a burglar may try to cover up evidence of his crime, so have terrorists, smugglers, et al, that depend on telephonic communications to ply their trade learned to cover up their electronic tracks. Some of the techniques they use are very basic and some are quite involved and sophisticated. Even some of the tricks that are easiest to apply are effective - very effective - so much so that it is not unusual for investigators to miss them.

For instance, did you know it is possible to make free telephone calls from a pay phone to anywhere in the country with no record of the call being stored anywhere? Can you believe that a phone call made from your bad guy’s monitored phone could, with careful manipulation by the target, show on your pen register that he dialed the local church's telephone number and talked for five minutes, when he actually called a number in Pakistan? These are just two of many tricks we have seen bad guys use to avoid detection of calls. Topics include in-depth examination of “creative” uses of landline, cell, pager, commercial PBX/CENTREX, and Internet accounts and services to mask calls pertinent to criminal activity.

This class covers the detection and identification of calls made using the "Tricks". Each of the Tricks and the accompanying ideas for countermeasures are explained in detail. Where appropriate, special verbiage for subpoenas and court order applications is presented to either preclude implementation of the trick or allow investigators access to true call information generated by the trick. The class also includes how to use the fact that your target is deliberately trying to avoid call detection to establish/add to your probable cause for a Title III and/or further law enforcement action.

Prepaid Calling Cards

With the advent of universally available prepaid telephone calling cards, it appears that telephone technology is working for the bad guys and working against the good guys. The bad guys use the cards to make calls over cell phones, pay phones, a friend's phone, etc. They know that investigators usually miss detection of calls made with prepaid cards. They know that when a calling card is used from a home phone to call either a long distance or local number, the toll-free access number (800, 888, 877, etc.) will never show on his phone bill, much less the actual call itself. The only chance we have to catch him is if we have a DNR on his line. But if he suspects that we may be monitoring him, all he has to do is make the call from a phone that is typically immune from monitoring - a randomly chosen pay phone, a "borrowed" phone, a company phone, etc.

Compounding the problem is the requirement (or what is generally accepted to be the requirement) to specify a telephone number on a subpoena or court order application. But we know that a single calling card can be, and usually is, used to make calls from several different telephones (and, for that matter, by more than one person) before it is used up.

The bad guys think that their calls are effectively insulated from law enforcement if they make them with a prepaid calling card. And, for all practical purposes, they are right. We in law enforcement have too often thrown up our hands when prepaid cards are used, figuring that the calls are "lost". Complicating matters, calling card providers are willing accomplices to the game. AT&T stopped passing actual caller ID on calls made using AT&T prepaid cards and now passes a “bogus” CallerID to confuse the recipient of the call. They did this because (as an AT&T security official said off-the-record) “… one of the reasons people buy our cards is to remain anonymous – and to sell in this market, we have to sell anonymity…”

The detection and identification of calls made with a prepaid card can be done using the methods covered in the class. This class will focus on all the ways prepaid cards are used by targets of investigation and discuss specific procedures to identify if a card is being used and how to reliably obtain call information from calls made on the card. Specific analytical techniques are covered using Microsoft Excel spreadsheets. Properly applied, these methods ensure that virtually no prepaid card calls can be lost to a determined investigator.

“Throw-Away” cell phone & Prepaid Calling Card Sting Operations

This is an intense session on how to set up sophisticated and effective throw-away cell phone and prepaid card sting operations for under $100 and then expand to as big an operation as needed at minimal cost. No technical know-how is necessary – all the information you need is presented in class. All concepts presented are adaptations of standard investigative and analytical techniques.

The bad guys are taking advantage of universally available throw-away cell phones and prepaid telephone calling cards they can purchase at the local Wal-Mart to make calls. They know that calls made with throw-aways and prepaid calling cards can be difficult to trace, particularly if they buy them from a store while we are not watching. To make the trail even more difficult to follow, they’ll use the same card from a many different telephones or, in the case of throw-away cells, literally throw them away and get a new one every month or so! The best way to win is to beat them at their own game. They want to use throw-aways and prepaid cards – so let them – but you will supply the phones and cards. This seminar combines training in the use of the latest technologies, provides knowledge and experience in dealing with these telephonic communication modes, and exploits an agent's creativity as applied to UC operations to close this loophole. Everything you need to know about purchasing phones and purchasing cards, or making your own cards with your own logo, getting them into the hands of the bad guys, and then capturing every call they make is covered. We will even cover how to employ the “use-a-phone/card-to-catch-a-phone/card” methodology, where seed phones and cards supplied by your covert operation can be used to identify and obtain call information on the phones and cards they purchase themselves.

Techniques presented include not only the distribution, tracking, and exploitation of card call detail records, but also how to run Title III monitoring of conversations made by targets while using the supplied phones and prepaid cards. In the case of prepaid cards, audio interception of calls is possible even if the target is calling from one foreign country to another foreign country, and can be done since the call audio on the prepaid cards recommended passes through the United States.

Writing Telephone Subpoenas & Court Order Applications

Before you can begin to analyze telephone call information, it is first necessary to obtain the telephone call information needed for the analysis. On the surface, this seems like an obvious and overly simplistic statement, but it's not. The key words "information needed for analysis" can make the difference between progress in your investigation or ineffective and sometimes

misleading analytical results. When writing a subpoena or affidavit, you need to keep in mind the basic principal, "if you don't ask for it, you won't get it". This also implies that you need to know what is available (i.e., what you can ask for) and how to ask for it.

Many agencies have boilerplate verbiage to be used in writing subpoenas and affidavits. Many times these "go-bys" will be adequate, but due to changing technology and the availability of new types of information, the boilerplate you used last year may not include some of this information and you'll lose it. The sad part is that you may never know what you lost – the phone company probably won't tell you - they regard subpoenas and court orders as a necessary evil and are not about to create more work for themselves.

The information presented in this seminar is not represented to include all details necessary for the preparation of the administrative subpoenas and/or court order applications/affidavits for telephone call and account details. It is assumed that you already have and understand the general language for the specific subpoena or court order application you intend to write. This class covers the fine points of what you need to know (in layman's language) about the new technologies and requirements as well as sample verbiage that gets you all the information you need to support your investigation.

Tracing Telephone Contacts to Locate Callers

This class is designed to provide the investigator with the basic procedural tools, techniques, sources, and legal basis to perform necessary initial action and to acquire and effectively use telephone contact and subscriber information to support the location and identification of callers. It covers…

1. Coordination of potential lead sources to obtain telephone information
2. Monitoring telephones that might be used by the or perpetrator
3. Consensual and non-consensual monitoring of call detail records
4. How to trace use of pay phones
5. Obtaining telephone CDR and Subscriber information
6. Using special telephone company databases to key in on the caller
7. Detecting/exploiting the use of cell phones, prepaid cell phones, and prepaid calling cards
8. Geographic location of cell phones
9. Identifying bogus 911 calls
10. Tracing calls to law enforcement tip lines

Telephone “Short Subjects”

Setting up and using "Hello" phones: A hello phone is a telephone used in covert law enforcement operations for communication with bad guys. It gets its name from the manner in which it is used. When the phone rings, instead of answering, "XYZ Office of Criminal Investigations", it is answered "hello".

Hello phones can be located anywhere, at an agency office or at an off-site where undercover investigators meet with and communicate with targets of investigation. To ensure that the bad guys don't suspect that the phone is subscribed to by a law enforcement agency, certain precautions are necessary. This class reviews how to set up service for the hello phone and how to insulate the phone from discovery. The training covers whom to call, what to say, how to maintain the service, and special equipment and features to subscribe to for your "hello" line. It also includes specific case examples of the consequences suffered by those who didn’t set up their "hello" phones properly and were either identified or whose operation was otherwise compromised, and how to avoid those pitfalls.

Dealing with "Phone Shy" bad guys: We've all run into them – bad guys that, for one reason or another, are afraid to use the telephone. You can spot them pretty easily. Sometimes they have no identifiable long distance landline service, or they keep "checking" for a wiretap, using whatever rumored method is popular at the time. Or they make calls, but never call criminal associates. This class covers how to identify them and how to get past their defensive communications shield.

NTI training can be customized for your agency. The following pages show sample past schedules for three, four, and five-day training courses incorporating the above training agenda…

Enhancing Investigations With Telephonic Information…3-Day

Bob Lottero, Instructor, NTI Law Enforcement Services, PO Box 99, Jefferson, NH 03583

Date/time		**Focus Areas**	**Topics to be Covered**
Day 1			
	0800-0830	Introduction	How tel info can enhance your investigation
	0830-0930	Telco Infrastructure	How telephone systems work… landline, cell,
			VoIP, PBX, CENTREX, toll-free, 900, satellite
	0930-1200	Countering criminal tricks to hide calls	Dial 0, Info connect, ppd cards & phones, collect,
			voice dial, pass-through, SIM swap, & more…
	1200-1300	***Lunch***	
	1300-1600	Subpoenas & Subpoena management and	Subscriber subpoena verbiage, investigative use
		how to exploit subscriber and CDR info	of subscriber records. CDR subpoena verbiage,
		to support your investigations	managing subpoenas, special subpoenas
	1600-1700	Court orders	Using subpoenaed subscriber & toll analysis to
			establish PC for a court order, writing the demand
			part of a court order, blocking potential tricks
Day 2			
	0800-1000	Tracing threat, harassment, 911, etc. calls	Little known techniques to ID callers
	1000-1200	Exploiting prepaid telephone calling cards	Using these strategies, you'll never lose a call
	1200-1300	***Lunch***	
	1300-1500	Exploitation of throw-away cell phones	ID subscribers, get the CDRs, monitor audio
	1500-1700	Sting & special operations	Setting up "hello" phones & toll-free numbers to
			support your case, conning the bad guys with a
			answering machine, putting prepaid cards & cell
			phones in the bad guys' hands all set to monitor!
Day 3			
	0800-0900	Exploitation of prison telephone systems	Add a proactive component to your prison work
			to identify criminal and terrorist activity
	0930-1200	Case Studies	How would you approach the telephonic aspect
			of these cases? An in-depth application of the

			investigative concepts presented in this course
	1200-1300	***Lunch***	
	1300-1500	Case Studies (continued)	
	1500-1700	Wrap-up, Questions, Discussion	

Enhancing Investigations With Telephonic Information… 4-Day

Bob Lottero, Instructor, NTI Law Enforcement Services, PO Box 99, Jefferson, NH 03583

Date/time		**Focus Areas**	**Topics to be Covered**
Day 1			
	0800-0830	Introduction	How tel info can enhance your investigation
	0830-0930	Telco Infrastructure	How telephone systems work… landline, cell,
			VoIP, PBX, CENTREX, toll-free, 900, satellite
	0930-1200	Countering criminal tricks to hide calls	Dial 0, Info connect, ppd cards & phones, collect,
			voice dial, pass-through, SIM swap, & more…
	1200-1300	***Lunch***	
	1300-1600	Subpoenas & Subpoena management	Subscriber subpoena verbiage, investigative use
			of subscriber records. CDR subpoena verbiage,
			managing subpoenas, special subpoenas
	1600-1700	Court orders	Using subpoenaed subscriber & toll analysis to
			establish PC for a court order, writing the demand
			part of a court order, blocking potential tricks
Day 2			
	0800-1000	Tracing threat, harassment, 911, etc. calls	Special searches few investigators use
	1000-1200	Exploiting prepaid telephone calling cards	Using these techniques, you'll never lose a call
	1200-1300	***Lunch***	
	1300-1500	Exploitation of throw-away cell phones	ID subscribers, get the CDRs, monitor audio
	1500-1700	Sting & special operations	Setting up "hello" phones & toll-free numbers to
			support your case, conning the bad guys with a
			answering machine, putting prepaid cards & cell
			phones in the bad guys' hands all set to monitor!
Day 3			
	0800-0900	Exploitation of prison telephone systems	Add a proactive component to your prison work
	0900-1200	Preparation of CDR paper and data files	Converting and reformatting paper, electronic tolls,
			and print-image tolls in any form to something you
			can use either in a commercial telephone
			analytical database or in Microsoft Excel
	1200-	***Lunch***	

	1300		
	1300-1700	CDR analysis	A DNR/pen instrument captures all digits dialed
			by a target; here's how to break them down & ID
			the individual calls and messages for analysis.
			CDR in-depth analysis - all analytical reports and
			techniques explained and utilized to produce leads
Day 4			
	0800-0930	Reading/using CALEA call event records	How to reduce the complicated CALEA messaging
			to a level that can be used efficiently on your case
	0930-1200	Case Studies	How would you approach the telephonic aspect
			of these cases? An in-depth application of the
			investigative concepts presented in this course
	1200-1300	***Lunch***	
	1300-1500	Case Studies (continued)	
	1500-1700	Wrap-up, Questions, Discussion	

Enhancing Investigations With Telephonic Information… 5-Day

Bob Lottero, Instructor, NTI Law Enforcement Services, PO Box 99, Jefferson, NH 03583

Date/time	Focus Areas	Topics to be Covered
Day 1		
0800-0830	Introduction	How tel info can enhance your investigation
0830-0930	Telco Infrastructure	How telephone systems work… landline, cell,
		VoIP, PBX, CENTREX, toll-free, 900, satellite
0930-1200	Countering criminal tricks to hide calls	Dial 0, Info connect, ppd cards/phones, collect,
		voice dial, 911 CID block, SIM swap, & more…
1200-1300	***Lunch***	
1300-1500	Tracing threats, 911, harassing, etc. calls	Special searches few investigators use
1500-1700	Exploiting prepaid telephone calling cards	Using these techniques, you'll never lose a call
Day 2		
0800-1000	Exploiting prepaid telephone calling cards	Continued
	(hands on computer)	
1000-1200	Exploitation of throw-away cell phones	ID subscribers, get the CDRs, monitor audio
1200-1300	***Lunch***	
1300-1500	Sting & special operations	Setting up "hello" phones & toll-free numbers to
		support your case, conning the bad guys with a
		answering machine, putting prepaid cards & cell
		phones in the bad guys' hands all set to monitor!
1500-1600	Exploitation of prison telephone systems	Add a proactive component to your prison work
1600-1700	Reading/using CALEA call event records	How to reduce the complicated CALEA messaging
Day 3		
0800-0930	Subscriber Subpoenas	Subscriber subpoena verbiage, investigative use
		of subscriber records
0930-1130	CDR subpoenas	Using the right words in your subpoena to get
		call detail records
1130-1200	Subpoena composition & management	Taking control of the subpoena process
	(hands on computer)	
1200-1300	***Lunch***	
1300-1400	Court orders	Using subpoenaed subscriber & toll analysis to

		establish PC for a court order, writing the demand
		part of a court order, blocking potential tricks
1400-1700	Preparation of CDR paper and data files	Converting and reformatting paper, electronic tolls,
	(hands on computer)	and print-image tolls in any form to something you
		can use either in a commercial telephone
		analytical database or in Microsoft Excel
Day 4		
0800-1000	Parsing dialed strings	A DNR/pen instrument captures all digits dialed
		by a target; here's how to break them down & ID
		the individual calls and messages for analysis.
1000-1200	Introduction to CDR analysis	Concepts and methodologies of call detail record
		analysis
1200-1300	***Lunch***	
1300-1700	CDR analysis	CDR in-depth analysis - all analytical reports and
	(hands on classroom)	techniques explained and utilized to produce leads
		that can be used on your case
Day 5		
0800-1200	Presenting your leads	Using tables and graphics to present and
	(hands on computer)	understand what you have found in your analysis
1200-1300	***Lunch***	
1300-1600	Case Studies	How would you approach the telephonic aspect
		of these cases? An in-depth application of the
		investigative concepts presented in this course
1600-1700	Wrap-up, Questions, Discussion	