

Fuller, Amber

From: Knight, Shawn
Sent: Tuesday, July 20, 2010 1:07 PM
To: Lindsey, Drennon
Subject: ESU
Attachments: ESU into OPD.doc

Good luck Lt. I hope you can get further with it then I could.

Thanks

Shawn

CITY OF OAKLAND

Memorandum

TO: Office of Chief of Police
ATTN: Chief Anthony W. Batts
FROM: Sergeant Shawn Knight
DATE: 16 Mar 10

RE: Implementation of ESU into the Oakland Police Department

The utilization of technology in law enforcement has become increasingly relied upon within the last couple of years. The progressive advancements made with this technology, such as PEN registers, Stingrays, and global positioning systems has allowed for the monitoring, tracking, and apprehension of criminals to become much more efficient and timely. The Oakland Police Department began implementing and using electronic surveillance equipment in 2001 and it has been used to assist the Fugitive Task Force and Targeted Enforcement Task Forces (TETF 1 and 2) to arrest some of Oakland's most violent offenders.

However, an Electronic Surveillance Unit (ESU) has not been established at OPD and with the increasing demand and workload involved to successfully expedite such systems; it is becoming a challenge and putting OPD at a disadvantage with combating crime. That is why I am proposing that the Oakland Police Department create an Electronic Surveillance Unit.

PAST CONFIGURATION:

Recently within the Criminal Investigation Division (CID), there were three specialized units that targeted major offenders and gangs. The Target Enforcement Task Forces (TETF I & II) and the Gang Investigations Task Force (GITF).

The primary responsibility of TETF I is to conduct covert investigations targeting major offenders wanted for crimes and or individuals/gang members involved in criminal activity.

The primary responsibility of TETF II was to assist the Homicide Section in locating witnesses and track down and arrest suspects wanted for homicide.

Although, the above two unit's responsibilities kept them incredibly busy, they were often tasked with additional requests from other sections, such as Robbery, Assault and SVU, for assistance in locating and arresting subjects. It should be noted that 75% of the time TETF I & II operated together as one unit. This was because of the nature of conducting these operations consisted of covert surveillance, used for locating suspects and or targets, and arrest teams, needed to make the arrest or identify subjects when need be. TETF I is partnered up with the FBI, often making their focus on Violent Crime Major Offenders (VCMO), and Gangs. The TETF 2 was recently disbanded to support patrol.

The primary responsibility of the GITF is to identify, locate and investigate gangs and their members in regards to their criminal activity. GITF is partnered up with the Alcohol Tobacco and Firearms (ATF), often making their focus into the recovery of firearms.

Mixed within both TETF Units was the small contingency of ESU officers. They use ESU technology on a daily basis, whether it is writing the court orders for ESU operations, analyzing the information collected, and operating/maintaining the different equipment used in ESU operations. ESU officers also operate and maintain the tactical electronic surveillance equipment used by our Department. It should be noted that ESU officers often assist all sections of the Oakland Police Department and outside agencies. ESU electronic case management technology is expected to be used in some upcoming major operations. ESU officers are always up-dating and maintaining the Department's wire room, keeping it ready at a moments notice; in the event such as the Kevin McDonald shooting or the Hasanni Campbell murder case arise.

I believe to properly use and maintain ESU technology our department needs to recognized and staff an Electronic Surveillance Unit. Below are some of the duties that ESU officers would be responsible for:

ESU DUTIES:

- ESU officers would be trained in writing court orders, to support all sections of the police department, involving Toll Records, Pen Registers, GPS Pings, Hemisphere requests and Wiretap Operations. Work associated with court orders requires having knowledge of the telephone service providers and the technology associated with those systems, the contact information, the CALEA process, and the data entry/set-up of the Lincoln Intercept System.
- ESU officers will be trained in Toll Analysis, Cell Site Analysis, and generate case packets associated with these reports.

- ESU officers will maintain and operate the Department's Lincoln System and its six intercept stations.
- ESU officers will be trained in maintaining and deployment of the Department's pole attic camera, under the door camera, thru-wall camera, crawl space camera and its command module monitoring station.
- ESU officers will be trained in maintaining and deployment of the Department's two surveillance robots, Recon Scout and Robotex Avatar.
- ESU officers will be trained in maintaining and deployment of the Department's Stingray van. This includes the operation system of GPS Microsoft Map Point, VisionTek, VPN remote viewing into the Lincoln System, Stingray System software, and operation of the battery bank inverter systems. It should be noted to become a Stingray operator takes a 40 hour course.
- ESU officers will be trained in maintaining and deployment of the Department's GPS vehicular tracking devices.
- ESU officers will be trained to deploy the Department's covert search kits.
- ESU officers will be trained to operate the Department's electronic case management Lincoln System. The officers will support pending wiretap operations and future projects. Case management duties include case Intel, research, data input, and generating reports associated with the projects.
- ESU officers will be trained to operate and manage the Department's CellBrite, cellular telephone forensics, system.
- ESU officers will support and work with the Intelligence Unit, I.A.D., CID, Patrol, and any other Department's sections, when requested to do so.

MANAGEMENT DUTIES:

- Management will be responsible for the day to day operations involving ESU personnel. The management must have knowledge and experience of all the listed systems. Management must know and have personal contact with the companies associated with the Department's operational systems, such as Harris Corp. "Stingray", Penlink Inc. "Lincoln System", Tracking the World "GPS Trackers" ETC. ETC. Management must be able to train new ESU members on the Department's operational systems.
- Management must track and maintain all costs associated with ESU operations and the yearly fees associated with the systems. Management must also research

and obtain funding and grants in order to maintain the systems, upgrade the existing systems, and the purchase of new equipment. Management must seek out new training for its members and the funding associated with those costs.

COLLATERAL DUTIES:

All ESU members will be trained and have knowledge of all resources available to them, in regards to any Departmental investigation. ESU members will be able to support any requesting Departmental section, in regards to the locating and apprehension of wanted subjects. ESU members will generate packets containing all material associated with wanted subjects. These packets will be made available to the requesting sections. The following are resources that ESU members will use: CORPUS, IIQ, MCMN, CRIMS, BOSS, LRMS, ENTERSECT, LEADS, FACEBOOK, MYSPACE, CABS, and ECT ECT.

ESU members will obtain knowledge and access on how to properly query these systems, in order to conduct proper investigations. ESU members will also have the knowledge in writing the court orders associated with the legal process in obtaining the requested information.

These skills, coupled with skills of ESU knowledge, will make ESU members a very valuable asset to the Department. The use of ESU personnel will be at the discretion of the Chief of Police.

I believe ESU personnel should be under the control of the Office of Chief of Police. Due to the time required to become sufficient in ESU operations, the contacts that are made and maintained over the years and the complexity of certain projects, ESU personnel should be placed in a no-cap assignment, such as the Intelligence Unit.

To date, there are two personnel trained in ESU operations, myself and Officer O. Crum. I would like to start this unit with two personnel and expand it in time, when resources and funding become more available.

It should be noted that two ex-TETF II personnel (Officers F. Bonifacio and J. Saunders) have some limited ESU training. I would like to continue to train these individuals and have the availability to have their assistance in the future, for any large or complex ESU operations. Also, I would like to use these individuals during the times that I or Officer O. Crum are not available.

PAST OPERATIONS:

Below are the listings of past cases, the crimes, and the outcome that the Department's informal ESU unit has been involved in:

OPERATION NUTCRACKER

Pen-Register/Wiretap	186.22 PC	Mark Candler	I/C
Pen-Register/Wiretap	186.22 PC	Kevin Reed	I/C
Pen-Register/Wiretap	186.22 PC	Marcel Perry	I/C
Pen-Register/Wiretap	186.66 PC	Ricky Daniels	I/C
Wiretap	186.22 PC	Purvis Ellis	I/C
Wiretap	186.22 PC	Donald Mills	I/C
Wiretap	186.22 PC	Dimari Marsh	I/C
Wiretap	186.22 PC	Lorenzo Morris	I/C

OPERATION FIND HASSANI

Pen-Register/Wiretap	207, 187 PC	Louis Ross	Not I/C (arrested/not charged pending further investigation)
----------------------	-------------	------------	--

FIELD OPERATIONS

Name	Crime	Technology used	Outcome\
Will Stallings	187(a), 211 207	PING	I/C, LA FBI
Derwin Upshaw	187(a) 245(b)	PEN, STNRY	I/C FBI Stnry Operation Atlanta, GA
Mathew McCall	187(a)	PEN	Self surrender
Daniel Stewart	261(a)(1) 266h, 211 266h(a) 209(b), 236	PEN, STNRY	I/C
Jesse Mendez	664/187(a) on	WIRE, PEN, STNRY	I/C, Sacramento Police officer
Demarkus Benavides	211	PEN, STNRY	I/C

Michael Campbell	187(a)	PEN	Not I/C
Juan Gonzales	187(a), 211 245(a)(2)	PEN, STNRY	I/C, Sacramento
Paul Moore	187(a)	PING	I/C, Antioch
Jaime Thomas	187(a)	PEN, STNRY	I/C, Modesto
Charome Davis	187(a)	PEN, STNRY	I/C, via DOJ Stury, San Diego
Marlon Campbell	245(a)(1) 207(a) 417(a)(2)	PING	I/C, via FBI Las Vegas
Kanika Jones	187(a)	PEN, STNRY	Not I/C, phone located Subject not in poss.
Phillip White	187(a)	PING	I/C, Denver PD
Richard Lewis	209(a), 206	PEN	Not I/C
Lloyd Townsend	187(a)	PEN, STNRY	I/C
Shareef Patten	187(a)	PING	I/C
Nathan Meredith	136.1(a)(1)	PEN, STNRY	I/C, Sacramento
Darryl Hill	187(a)	PEN, STNRY	I/C, Richmond
Dwayne Jackson	187(a)	WIRE, PEN	I/C, St. Louis, MI Via FBI
David Taylor	211	PEN, STNRY	I/C
Dimario Pickford	187(a)	PEN, STNRY	I/C
Reamel Curtis	211	PEN	I/C, VIA Sacramento PD
Terrell Stanford	192(a) 211	PEN, STNRY	I/C, Fairfield case
Dario Cannon	187(a)	PEN, STNRY	Not I/C
Delay Graham	211	PEN, STNRY	I/C

Anthony Ford	211	PEN	I/C, San Leandro case
Pablo Cervantes	245(c)	PEN, STNRY	I/C
Joshua Ropati	215	PEN, STNRY	I/C
Dwayne Robinson	187(a)	PEN, STNRY	I/C, Hayward
Curtis Powell	187(a)	PEN	Not I/C
Ryan Bradford	187(a)	PEN	I/C, Sacramento PD
Elliott Marshall	211, 212.5	PEN	I/C, Mendocino case
Jamel Curtis	246.3	PEN, STNRY	I/C, Alco case
Lincoln Terrance	211, 207	PEN, STNRY	I/C, Sunnyvale case
Pierre Goins	187(a)	PEN, STNRY	I/C, Stockton
Patrick Grant	211 on OPD Officer	PEN, STNRY	I/C, San Pablo
Laron Logwood	187(a)	PEN, STNRY	I/C, Berkeley
David Denson	187(a) X 2 245(a) (2)	PEN, STNRY	I/C, San Leandro, Sacramento PD case
Eseta Penitani	187(a)	PEN	I/C, San Leandro
Joel Barnes	245(b)	PEN, STNRY	I/C, Watsonville, Santa Clara case
Toure Clayton	207	PEN, STNRY	I/C, Sacramento, Sacramento case
Damon Ferreira	187 X 2 245(a) (2)	PEN	I/C/DOA, Stockton
Ronald Thomas	187(a)	PEN, STNRY	I/C, Richmond
Jason Kaufman	187(a)	PEN, STNRY	I/C

From Sept. 2006 to present, ESU technology has been responsible for 39 violent suspects being taken into custody. Many of these cases involved very fast captures, saving the Department thousands of dollars in fugitive investigations. Also, many of the captures were outside the city of Oakland, which in the past has been problematic in obtaining out of agency cooperation. Using ESU technology during investigations prevents time consuming remote investigations, prior to being able to conduct a surveillance operation.

Six cases have not resulted in an "in-custody status". This is due to two self surrenders, three dropped phones and one phone located, but not with the listed suspect.

It should also be noted that an ESU investigation, involving the preparation and proper planning, has prevented any OPD officers from being injured during any ESU operations.

Sgt. S. Knight
BOI-CID
510/238-3640

Fuller, Amber

From: Poulson, Edward
Sent: Wednesday, September 29, 2010 12:39 PM
To: Knight, Shawn
Subject: RE: Grant

Shawn,

Candise has left the department and with her the information. I don't have it. Maybe check with Ms. Silva in Fiscal. Just clearing out old e-mail.

Ed

From: Knight, Shawn
Sent: Thursday, July 29, 2010 6:08 PM
To: Poulson, Edward
Subject: RE: Grant

Can I get a copy for future use. I like having go-byes, it makes it easier when situations like these come by.

Thanks

From: Poulson, Edward
Sent: Thu 7/29/2010 6:07 PM
To: Knight, Shawn
Subject: RE: Grant

Yes.

From: Knight, Shawn
Sent: Thursday, July 29, 2010 6:06 PM
To: Poulson, Edward
Subject: RE: Grant

I take it that somebody wrote up the proposal for that?

From: Poulson, Edward
Sent: Thu 7/29/2010 6:01 PM
To: Knight, Shawn
Subject: RE: Grant

Not getting anything yet. If all goes well, it will be a new CAD, report writing software, something for crime analysis that D/C Israel wanted, and new laptops for every vehicle that works on the street.

From: Knight, Shawn
Sent: Thursday, July 29, 2010 5:57 PM
To: Poulson, Edward
Subject: RE: Grant

Capt.

Just out of curiosity, what technological equipment are we getting for patrol?

From: Poulson, Edward
Sent: Thu 7/29/2010 3:17 PM
To: Knight, Shawn
Subject: RE: Grant

Shawn,

I submitted the paperwork. The COP wanted to go with equipment for patrol.

Ed

om: Knight, Shawn
Sent: Tuesday, July 27, 2010 2:59 PM
To: Poulson, Edward
Subject: Grant

Capt.

I was just wondering if there is any update on that Grant proposal I submitted several weeks ago?

Thanks

Shawn

Fuller, Amber

From: Knight, Shawn
Sent: Thursday, August 05, 2010 9:35 AM
To: Poulson, Edward
Subject: RE: Grant

Capt. any luck yet?

From: Poulson, Edward
Sent: Thu 7/29/2010 6:10 PM
To: Knight, Shawn
Subject: RE: Grant

Let me see if I can get it.

From: Knight, Shawn
Sent: Thursday, July 29, 2010 6:08 PM
To: Poulson, Edward
Subject: RE: Grant

Can I get a copy for future use. I like having go-byes, it makes it easier when situations like these come by.

Thanks

From: Poulson, Edward
Sent: Thu 7/29/2010 6:07 PM
To: Knight, Shawn
Subject: RE: Grant

Yes.

From: Knight, Shawn
Sent: Thursday, July 29, 2010 6:06 PM
To: Poulson, Edward
Subject: RE: Grant

I take it that somebody wrote up the proposal for that?

From: Poulson, Edward
Sent: Thu 7/29/2010 6:01 PM
To: Knight, Shawn
Subject: RE: Grant

Not getting anything yet. If all goes well, it will be a new CAD, report writing software, something for crime analysis that D/C Israel wanted, and new laptops for every vehicle that works on the street.

From: Knight, Shawn
Sent: Thursday, July 29, 2010 5:57 PM

To: Poulson, Edward
Subject: RE: Grant

Capt.

Just out of curiosity, what technological equipment are we getting for patrol?

From: Poulson, Edward
Sent: Thu 7/29/2010 3:17 PM
To: Knight, Shawn
Subject: RE: Grant

Shawn,

I submitted the paperwork. The COP wanted to go with equipment for patrol.

Ed

om: Knight, Shawn
Sent: Tuesday, July 27, 2010 2:59 PM
To: Poulson, Edward
Subject: Grant

Capt.

I was just wondering if there is any update on that Grant proposal I submitted several weeks ago?

Thanks

Shawn

Fuller, Amber

From: Knight, Shawn
Sent: Monday, August 16, 2010 11:40 AM
To: Tull, Steven

Capt.

Here are the yearly maintenance fees for the Stinray and the Lincoln intercept system. Also, a projected budget for a years worth of Pen registers, Pinging and other costs associated with ESU.

Lincoln	\$34,000
Stingray	\$11,000
ESU costs	\$40,000
 Total	 \$85,000

Thanks

Shawn

Fuller, Amber

From: Knight, Shawn
Sent: Thursday, September 23, 2010 3:19 PM
To: Eric Ivers
Subject: RE: Robot repairs

Eric,

Sounds great. We were planning on coming down on Tuesday anyway. We found out Tuesday that our gears are stripped again somehow. Anyway I'll call you next week.

Thanks

Shawn

From: Eric Ivers [<mailto:eric@robotex.us>]
Sent: Thu 9/23/2010 2:00 PM
To: Knight, Shawn
Subject: Robot repairs

Hey, Shawn, why don't you guys bring the robot down next week and let us update it? We'll put a p/t/z back on it and fix anything else that's wrong with it.

Eric

Fuller, Amber

From: Knight, Shawn
Sent: Monday, September 27, 2010 2:04 PM
To: Burke, Dave
Subject: RE: Requested information on the Avatar robot that your SWAT Team is currently using.

Dave..

I'll take care of it.

Shawn

From: Burke, Dave
Sent: Fri 9/24/2010 10:59 AM
To: Crum, Omega; Knight, Shawn
Subject: FW: Requested information on the Avatar robot that your SWAT Team is currently using.

Geek squad can you guys handle this request for me. Thanks

From: Bruce.Theusch@co.washington.wi.us [mailto:Bruce.Theusch@co.washington.wi.us]
Sent: Thursday, September 23, 2010 6:28 PM
To: DL - OPD - ITU
Subject: Requested information on the Avatar robot that your SWAT Team is currently using.

Hello,

I was wondering if you could provide contact information for one of your personal that would be responsible for maintaining and operating your Robotex Avatar Micro robot. We are looking a purchasing a robot in the near future.

Thank you for any information that you can provide.

Lt. Bruce Theusch
Washington County Sheriff's Dept.
500 N. Schmidt Rd P.O. Box 1986
West Bend WI 53095
Phone (262) 335-4403
Fax (262)335-4429

The information in this email, and any attachments, may contain confidential information. Use and further disclosure must be consistent with applicable laws. However, if you believe you've received this email in error, delete it immediately and do not use, disclose or store the information it contains.

Fuller, Amber

From: Downing, David
Sent: Wednesday, June 09, 2010 4:03 PM
To: Knight, Shawn
Subject: RE: Robot

Shawn,

I sent the request to the Chief's Office. This is what they want before approval. A hard copy document--inter office letter--describing what they want and how they have benefitted us. Such as the gift of the robot, the continued maintainance, technical assistance and free upgrades. Try and put a price value on each one. Then send it to me for approval and I will forward through chain of command. Keep it to one page. You can put it in my in-box in my office out at Eastmont. The door is unlocked so just go in and leave it. I will take care of it when I get back Tuesday. I don't see a problem with the request and I will support it since they have really helped us out with the technology.

Dave

From: Knight, Shawn
Sent: Wed 6/9/2010 8:39 AM
To: Downing, David
Subject: Robot

Capt.

The makers of our robot "RoboteX" wants to use some pictures of me and Omega deploying our robot, for their website I have informed them and they understand that any pictures of our patches and or the identification of the Oakland Police Department would have to be approved by the Departmental prior to any use. Also, if possible I would like them to come to one of our tactical training days, so if approved, they can get some pictures deploying the robot with the Bear Cat and additional teams members.

Thanks

Shawn

Fuller, Amber

From: John Cassani <jcassani@lncurtis.com>
Sent: Friday, July 16, 2010 1:44 PM
To: Knight, Shawn
Subject: FW: trkg#

Sgt Knight,

The Zistos charger is on it's way.

The robot charger to Oakland is shipping out today UPS 3 day
UPS Tracking#
1ZY808351292969083

Regards,

John Cassani

L.N.Curtis&sons

1800 Peralta St.
Oakland, Ca. 94607
ph. (510)268-3305
fax (510)839-5325

"Knowledge is Power"

VISIT: <http://www.firebooks.com>

The FireFighters Bookstore

From: A.J. Paugh [<mailto:apaugh@zistos.com>]
Sent: Friday, July 16, 2010 1:39 PM
To: 'John Cassani'; pkurpinsky@lncurtis.com
Subject: FW: trkg#

Oakland PD's charger

A.J. Paugh
+1 631-434-1370 x308 office
+1 631-434-9104 Fax
[REDACTED] Mobile
www.zistos.com

From: Hassan Cheikhali [<mailto:hcheikhali@zistos.com>]

Sent: Friday, July 16, 2010 4:31 PM

To: 'A.J. Paugh'

Subject: trkg#

AJ,

The robot charger to Oakland is shipping out today UPS 3 day

Tracking#

1ZY808351292969083

Regards,

Hassan

Fuller, Amber

From: John Spomer <jspomer@penlink.com>
Sent: Tuesday, July 27, 2010 1:31 PM
To: Knight, Shawn
Subject: Grant for Pen-Link / CIA Conference
Attachments: Oakland PD-Replacement Hardware & Maintenance.doc

Hey Shawn,

Are you hearing anything yet regarding the status of your grant for replacement hardware and maintenance?

On a different subject, I'm also trying to remind all of our LINCOLN customers of this year's CIA conference which is scheduled for 8/31 - 9/1 in Lincoln. The following link has more information on this year's conference.

www.penlink.com/cia

Let me know if works for you or anyone else from Oakland to attend.

Thanks,

John



John Spomer | Sr. Sales Executive
5936 VanDervoort Drive | Lincoln, NE 68516 | USA
402.421.8857 Office | 402.202.3500 Cell | 402.421.9287 Fax
jspomer@penlink.com | www.penlink.com

From: John Spomer
Sent: Friday, June 11, 2010 4:52 PM
To: 'sknight@oaklandnet.com'
Subject: Quote

Shawn,

Attached is a quote to replace your LINCOLN system hardware and extend your maintenance for another 3 years. I'm in the office all day on Monday, so call if you have any questions or need me to make changes.

Thanks,

John

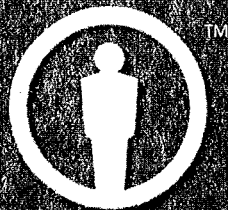


John Spomer | Sr. Sales Executive

5936 VanDervoort Drive | Lincoln, NE 68516 | USA
402.421.8857 Office | 402.202.3500 Cell | 402.421.9287 Fax
jspomer@penlink.com | www.penlink.com

Learn about the 2010 Pen-Link CIA Conference at www.penlink.com/cia

CONFIDENTIALITY NOTICE: The information in this email is confidential proprietary property of Pen-Link, Ltd. Unauthorized use of this communication is strictly prohibited and may be unlawful. If you have received this communication in error, please immediately notify the sender by reply email and destroy all copies of the communication and any attachments.



PEN • LINK™

It's the Key™

LINCOLN Intercept System End of Life Cycle Hardware Refresh & Extended Premium Maintenance Proposal

Prepared for:

Oakland Police Department

Point of Contact:

John Spomer
Sr. Sales Executive
jspomer@penlink.com

Pen-Link, Ltd.
5936 VanDervoort Dr.
Lincoln, NE 68516

Phone: (402) 421-8857
FAX: (402) 421-9287
Cell: (402) 202-3500

Revision 01
June 11, 2010

Pen-Link, Ltd. is a
U.S. - Based Small Business

DUNS: 195956636
TIN: 47-0707585
CAGE: OK6H9



PEN·LINK

It's the Key™

01/5/11/12/1

The following is a quote to refresh the hardware for Oakland PD's 6-channel, 9-user LINCOLN system.

Pen-Link Ltd. recommends to its customers that they periodically replace system hardware. Oakland PD's original LINCOLN system was shipped in May 2006 and the hardware for the system is now over 4 years old and is no longer covered under warranty. Improved system performance and the ability to support MapPoint Cell Tracking Software and Pen-Proxy Services are benefits to refreshing system hardware.

Quantity	Description	Unit Cost	Total Cost
1	LINCOLN Recording Server <ul style="list-style-type: none">• Includes Dual Quad Core Processors• 6 GB RAM• (4) 300GB 15k RPM Hard Drives, Redundant Power Supply• Perc 6/i Raid Controller• Redundant Power Supplies• Dual Embedded Broadcom® NetXtreme II 5708 Gigabit Ethernet NIC• Rack Chassis w/Rapid Rails• CD-RW/DVD-ROM• 3 Year Next Business Day Support• Windows Server 2008 Standard• (10) Windows Server Device CAL• PC Anywhere• Dialogic 12 Port Analog• (6) Dialogic Line Runtime License• (2) Eicon 4 Port ISDN Card (For Nextel)• (6) Eicon NT1's	\$19,462	\$19,462
1	Pen-Link Server <ul style="list-style-type: none">• Dual Quad Core Processors• 6 GB RAM• (4) 300 GB 15K SAS Hard Drives• Perc 6/1 RAID Controller• Redundant Power Supplies• Dual Embedded Broadcom NetXtreme II GB NIC• Rack Chassis w/Rapid Rails• CD-RW/DVD-Rom• Windows Server 2008 Standard• PC Anywhere• 3 Year Warranty	\$9,451	\$9,451



PEN·LINK

It's the Key™

1	Rack and UPS's <ul style="list-style-type: none">• Dell 42U Rack• 17" KMM• 3 Fixed Shelves• 3 Year Warranty• KVM - 4 Port• (2) KVM Cables – 15 Foot• (2) APC RM PDU 1U• (2) APC 1500 UPS• Misc Cabling• Cat 5E 48 Port Patch Panel	\$6,211	\$6,211
9	Workstations <ul style="list-style-type: none">• Core 2 Duo 2.33 GHz Processor• 4 GB RAM• 250 GB SATA Hard Drive• DVD-RW• Dual 19 inch Flat Panels with 256MB Graphics Card• AS501 Soundbar• 3 Year NBD Support• Labtec Elite Headphones• Infinity USB Footpedal• APC SmartUPS 1300VA - Workstations	\$2,642	\$23,778
9	MapPoint Software	\$500	\$4,500
1	Networking Equipment <ul style="list-style-type: none">• Dell PowerConnect 5324 24-Port Switch• (4) Zoom modems• Edgeport• CISCO VPN Router 5505 Package, 25 Tunnels (Includes 3 Year Warranty and 4 hours of Configuration Services)	\$6,150	\$6,150
1	Evidence Storage <ul style="list-style-type: none">• ProStor WORM RDX-10 System Package (Includes 3 year limited Warranty and (10) 80GB Cartridges)	\$14,823	\$14,823
1	LaserJet Color Printer	\$1,686	\$1,686
1	3-Days On-Site Installation (Price Includes Pen-Link's Travel)	\$10,000	\$10,000
1	3-Days On-Site Training CATS, PAC or LAT Format (Price Includes Pen-Link's Travel)	\$12,000	\$12,000
1	Premium Maintenance (Price Based on a 6 Channel / 8 User Configuration) for the term October 1, 2010 – September 30, 2012	\$99,656	\$99,656
	TOTAL		\$207,717



PEN·LINK™

It's the Key™

- The pricing for this quote is valid until August 11, 2010.
- Acceptance of this proposal by the issuance of a purchase order or letter of intent signifies the customer agrees to the terms and conditions of "Pen-Link, Ltd. Maintenance and Support Terms and Conditions".

Pen-Link, Ltd. Maintenance and Support Terms and Conditions

1. Terminology

The following terms and definitions apply throughout this document.

- 1.1. **Pen-Link Software.** Pen-Link Software is software that is developed and manufactured by Pen-Link, Ltd.
- 1.2. **Pen-Link Customer** (also "Customer"). A Pen-Link Customer, or Customer, is any agency or other entity that has one or more current, valid Licenses for Pen-Link Software that were purchased from or through Pen-Link, Ltd.
- 1.3. **Basic Technical Support Package.** Entitles our customers to normal business hours telephone support at Pen-Link, Ltd.'s published number, and/or assistance via e-mail.
- 1.4. **Standard Maintenance and Support.** Standard Maintenance is a Maintenance option that includes Software Updates, Software Upgrades, and Basic Technical Support as defined herein.
- 1.5. **Premium Maintenance and Support.** Premium Maintenance is a Maintenance option that includes Software Updates, Software Upgrades, and Premium Technical Support as defined herein.
- 1.6. **Software Update.** A Software Update is an enhancement—including additions, changes, and bug fixes—to Pen-Link Software that is already in the applicable commercial market. Software Updates occur within the same major version number of an existing software product. For example, replacing Pen-Link v8.1.29.0 with Pen-Link v8.1.30.0 would constitute a Software Update. Such an update is often referred to as a "New Build" of the Pen-Link Software.
- 1.7. **Software Upgrade.** A Software Upgrade is the replacement of an older major version of an existing Pen-Link Software product or products, with a newer major version of a Pen-Link Software product or products, to the extent required to maintain the same operational functionality that was supported by the Pen-Link Software prior to the upgrade. For example, upgrading from Pen-Link Version 7 to Pen-Link Version 8 (where 8 is the newer major version) would constitute a Software Upgrade, so long as the installation of the newer version of the Pen-Link Software supported at least the same operational functionality that the Customer had under Pen-Link version 7. Upgrades do **not** apply to *new* software products that Pen-Link, Ltd. may release to the commercial market from time to time in the future.
- 1.8. **Basic Technical Support** (also "Basic Support"). Basic Technical Support is a Support option that includes telephone-based Technical Support for the Pen-Link Software licensed by the Customer. Basic Technical Support also includes assistance via email or other automated processes such as Pen-Link, Ltd. may deem fit to offer. Basic Technical Support may be obtained by contacting Pen-Link, Ltd. via its published, main telephone number (currently 402-421-8857), its general support email account (support@penlink.com), or its World Wide Web site (www.penlink.com). Basic Technical Support is available Monday through Friday, from 8:00 AM to 5:00 PM Central time, except for holidays.
- 1.9. **Premium Technical Support** (also "Premium Support"). Premium Technical Support is a Support option that includes all of the support services offered with Basic Technical Support (Section 1.8), plus Emergency After-Hours support for live communication interception and collection operations. Emergency After-Hours support services may be accessed through methods, including telephone access, that are provided to the customer at the time of purchase. Emergency After-Hours support services are available Monday through Sunday, from 5:01 PM - 7:59 AM Central time, including holidays.
- 1.10. **Maintenance and Support Agreement** ("Agreement"). This Maintenance and Support Agreement is the Agreement between Pen-Link, Ltd. and the Customer regarding the terms and conditions under which the Maintenance and Support Services described in this document are purchased and provided.

2. SOFTWARE MAINTENANCE ("MAINTENANCE")

- 2.1. Maintenance is an optional service offered by Pen-Link Ltd. to augment a purchase of Pen-Link Software. Maintenance may be purchased by a Pen-Link Customer along with, or subsequent to, the purchase of Pen-Link Software.
- 2.2. Maintenance is offered only pursuant to a Maintenance and Support Agreement between the Customer and Pen-Link, Ltd.



PEN·LINK™

It's the Key™

- 2.3. Pen-Link, Ltd. offers two levels of Maintenance that a Customer may purchase: Standard Maintenance and Premium Maintenance, as defined in Sections 1.4 and 1.5 respectively.
- 2.4. Maintenance applies only to software developed and manufactured by Pen-Link, Ltd. Maintenance does not apply to software developed and manufactured by companies other than Pen-Link, Ltd. Unless otherwise specified in a separate, written agreement between Pen-Link, Ltd. and the Customer, to which Pen-Link, Ltd. is a signatory party, Maintenance does not include updates, upgrades, or bug fixes to, or new releases of, any third-party software or hardware purchased through Pen-Link, Ltd. or with the assistance of Pen-Link, Ltd. Support for third party software and hardware products bundled with Pen-Link, Ltd. Licensed Pen-Link Software is available only according to the third-party manufacturer's support policies.
- 2.5. All Maintenance deliveries are subject to the terms and conditions of the applicable End User License Agreement ("EULA") for the Licensed Software.

3. TECHNICAL SUPPORT ("SUPPORT")

- 3.1. Technical Support ("Support") is an optional service offered by Pen-Link, Ltd. to support a Customer in the authorized use of licensed Pen-Link Software.
- 3.2. Support is offered only pursuant to a Maintenance and Support Agreement between the Customer and Pen-Link, Ltd.
- 3.3. Pen-Link, Ltd. offers two levels of Technical Support: Basic Technical Support and Premium Technical Support, as defined in Sections 1.8 and 1.9 respectively.
- 3.4. Pen-Link, Ltd. will make every reasonable attempt to answer a Customer's Support questions and address a Customer's Support concerns. However, Support is offered on a good faith, diligent effort basis only, and Pen-Link, Ltd. may not be able to resolve every request for Support.
- 3.5. Technical Support is provided for ongoing, operational use of the licensed Pen-Link Software; Support is not intended to be a substitute for training or professional services necessary for the implementation or system redesign of the licensed Pen-Link Software, which are outside the scope of this agreement. All such services, including without limitation, training, on-site assistance, consultation, custom programming and other software customizations, network design, and database and network administration, may be provided pursuant to separate agreements with and by Pen-Link, Ltd.
- 3.6. Unless otherwise specified in a separate, written agreement between Pen-Link, Ltd. and the Customer, to which Pen-Link, Ltd. is a signatory party, Support is available only for the current and immediately preceding version of the licensed Pen-Link Software. Support for a previous version of Pen-Link Software is provided up to a maximum of eighteen (18) months after the release of the current version of software, provided that the Customer and Pen-Link, Ltd. are parties to a current Maintenance and Support Agreement.
- 3.7. Unless otherwise specified in a separate, written agreement between Pen-Link, Ltd. and the Customer, to which Pen-Link, Ltd. is a signatory party, Support does not include any of the following:
 - 3.7.1. Support for database products or so-called "DBMS" or Database Management Systems, including without limitations, setup and alteration and/or configuration of such products, and resolution of errors related directly to such products.
 - 3.7.2. Resolving network, workstation, or other environmental errors not directly related to the licensed Pen-Link Software.
 - 3.7.3. Support for any licensed Pen-Link Software working on or with any version of any database, Database Management System, operating system, or other hardware or software product or system that is not specifically identified as interoperable and compatible with the specific version of the license Pen-Link Software being used.
 - 3.7.4. Support for any "alpha," "beta," or other preproduction release of any software, including Pen-Link Software.
 - 3.7.5. Support for any changes to Pen-Link Software made outside of the product's scope by a customer or by any third party.
 - 3.7.6. Support for any licensed Pen-Link Software that is used for a purpose, or in a manner, for which it was not designed.

4. TERMS AND CONDITIONS

- 4.1. Maintenance and Support Agreements are options made available by Pen-Link, Ltd for a Customer to purchase.
- 4.2. Maintenance and Support Agreements are offered on an annual basis.
- 4.3. Unless otherwise specified in a separate, written agreement between Pen-Link, Ltd. and the Customer, to which Pen-Link, Ltd. is a signatory party, Maintenance and Support Agreements will renew automatically at the end of each annual term, provided that the Customer pays the applicable renewal fees.
- 4.4. Unless otherwise specified in a separate, written agreement between Pen-Link, Ltd. and the Customer, to which Pen-Link, Ltd. is a signatory party, a Customer's Maintenance and Support Agreement is to be paid at the start of each annual term.
- 4.5. **Payment.** The Customer will be invoiced prior to any annual Maintenance and Support term (initial or renewal terms). The Customer agrees to make payment to Pen-Link, Ltd. no later than thirty (30) days from the date of the invoice, unless otherwise agreed upon in writing. Unless otherwise instructed, the Customer will make payment directly to Pen-Link, Ltd.



PEN·LINKSM

It's the KeySM

- 4.6. Pen-Link, Ltd.'s obligations hereunder are subject to the Customer's timely payment for Maintenance and Support. Failure of the Customer to pay fees in a timely manner for any term of Maintenance and Support may, at the sole discretion of Pen-Link, Ltd., result in the termination or suspension of Maintenance and Support services.
- 4.7. **Lapses and Reinstatement.** If a Customer's Maintenance and Support agreement terminates as a result of expiration or otherwise pursuant to this Agreement, and the Customer decides to reinstate the Agreement, the Customer will be required to pay the applicable Maintenance and Support fees for the lapsed period (the time elapsed between the Agreement expiring and subsequently being reinstated), plus a reinstatement fee equal to 10% of the fees for the lapsed period.
- 4.8. **Taxes.** The Customer is responsible for payment of all applicable taxes, value added taxes, or other taxes (however designated) related to the Maintenance and Support of the Licensed Software, unless otherwise agreed upon and stated in writing.
- 4.9. This Agreement will automatically terminate for each Licensed Pen-Link Software product upon termination of the EULA corresponding to such Pen-Link Software product.
- 4.10. The Customer may terminate this Agreement for Convenience, but the Customer will not be entitled to a refund of any paid fees in such an event.
- 4.11. **Additional Orders.** Orders by the Customer for additional Pen-Link Software products or additional licenses of Pen-Link Software products will increase the Customer's Maintenance and Support fees under this Agreement.

WARRANTY AND LIABILITY DISCLAIMER

- 5.1. Pen-Link, Ltd. warrants that the Maintenance and Support services provided to the Customer under this Agreement shall be performed with due care, and in a professional and workmanlike manner. Pen-Link, Ltd. does not otherwise warrant the accuracy or completeness of any services provided pursuant this Agreement. PEN-LINK, LTD. DISCLAIMS ANY AND ALL OTHER WARRANTIES, EXPRESS, IMPLIED OR OTHERWISE, IN CONNECTION WITH THE SUBJECT OF THIS AGREEMENT. IN NO EVENT, UNDER ANY THEORY OF LAW, SHALL EITHER PARTY AND/OR ITS AFFILIATES BE LIABLE TO THE OTHER FOR ANY INDEMNITY, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LOST PROFITS AND/OR ITS AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. PEN-LINK, LTD.'S. LIABILITY UNDER THIS AGREEMENT SHALL NOT EXCEED THE PREPAID AND UNUSED PORTION OF THE CUSTOMER'S MAINTENANCE AND SUPPORT FEES PAID TO PEN-LINK, LTD. PEN-LINK, LTD. SPECIFICALLY DISCLAIMS ALL RESPONSIBILITY FOR ANY SERVICES PROVIDED BY ANY PARTNER OR ANY OTHER THIRD PARTY.
- 5.2. It is the sole responsibility of the Customer to make and maintain adequate backup copies of software and data.
- 5.3. In no event will Pen-Link, Ltd. be responsible for lost data.

MISCELLANEOUS

- 6.1. **Entire Agreement.** This Agreement constitutes the entire Agreement between the Customer and Pen-Link, Ltd. related to the subject matter hereof, and additions or modifications shall be binding upon the parties only if the same shall be in writing and duly executed by the Customer and a duly authorized officer of Pen-Link, Ltd. The Licensed Pen-Link Software is licensed under a separate End User License Agreement (EULA) and professional services, if any, are provided under a separate professional services agreement. The terms and conditions of any Customer purchase order are only binding on Pen-Link, Ltd. if they are agreed to in writing by an authorized Pen-Link, Ltd. officer and in a document other than the purchase order.
- 6.2. **Waiver.** The waiver or failure of either party to exercise in any respect any right shall not be deemed a waiver of any further or future right.
- 6.3. **Assignment.** The Customer may assign this Agreement only in connection with a proper and valid assignment of the corresponding EULA to the extent permitted there under; provided that the Customer gives written notice of such assignment to Pen-Link, Ltd. Pen-Link, Ltd. may freely assign this Agreement to a purchaser of that portion of Pen-Link Ltd's. business to which this Agreement relates, to the surviving corporation in the event of a merger, and to any affiliate or third-party whom Pen-Link authorizes to provide Maintenance and Support for the Licensed Pen-Link Software of the nature contemplated hereby.

Fuller, Amber

From: Manu Singh <manusingh@gmail.com>
Sent: Tuesday, July 27, 2010 3:21 PM
To: Knight, Shawn
Subject: Re: Citation

You are right, this has already been paid. Please ignore this one but there is another one that was meant to send it to you.

<u>T1006566715</u>	CA 4XFB828	09-Jun-10 15:48:39	<u>RSR</u>	PAID COMPLETELY	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
[] <u>T1007542139</u>	CA 4XFB828	01-Jul-10 22:52:29	<u>RSR</u>	OPEN CITATION	\$5.00	\$25.00	\$0.00	\$0.00	\$0.00	\$30.00

On Tue, Jul 27, 2010 at 2:53 PM, Manu Singh <manusingh@gmail.com> wrote:
Shawn,
Let me check with fastrak and get back to you.

THanks
Manu

On Tue, Jul 27, 2010 at 2:48 PM, Knight, Shawn <SKnight@oaklandnet.com> wrote:
Manu,

These citations are the ones I sent the payment for two weeks ago.

Thanks

Shawn

From: Manu Singh [mailto:manusingh@gmail.com]
Sent: Tue 7/27/2010 2:23 PM
To: Knight, Shawn
Subject: Citation

Fuller, Amber

From: Brouhard, John, DA <john.brouhard@acgov.org>
Sent: Monday, August 02, 2010 7:22 AM
To: Chew, Craig, DA
Cc: Knight, Shawn
Subject: FW:

Craig --

Just a reminder. Please get this from Shawn this a.m. and get it to me. I need it before I can mark the exhibit containig all of the line sheets of Andrea Piazza. Thanks. messages.

-----Original Message-----

From: Brouhard, John, DA
Sent: Saturday, July 31, 2010 2:34 PM
To: 'Knight, Sgt. Shawn'
Cc: Chew, Craig, DA
Subject:

Shawn --

I am missing one line sheet for a text message: It is MAC with 302-5490, 05-12-08, 09:26:10, "Oh okay i needed that laugh right now to thanks even tho that kinda turne me on u never got at me like that"

Can you print this out Monday morning and get it to Craig?

Thanks again for finding all of this . . . you have no idea what a find this was!

John J. Brouhard
Deputy District Attorney
(510) 272-6275
john.brouhard@acgov.org

Fuller, Amber

From: Manu Singh <manusingh@gmail.com>
Sent: Monday, August 02, 2010 9:49 AM
To: Knight, Shawn
Subject: Smog
Attachments: ak05a4qr.pdf; ATT1042262.htm

Hi Shawn

Just for your reference, the officer might need this incase you guys decide to do the smog check.

-- Manu

Begin forwarded message:

From: MaxEmail <maxemail-bounce@maxemail.com>
Date: August 2, 2010 9:16:53 AM PDT
To: manusingh@gmail.com
Subject: 1 page MaxEmail fax from an unknown sender



You received a 1 page fax from an unknown sender on Mon, 2 Aug 2010 09:16:47 -0700. The message is attached to this email.

The reference number for this message is 8155508584-AK05A4QR.

A PDF viewer program is required to open and view this fax. Please visit the [MaxEmail software information center](#) for information about where to download software.

Please visit the [MaxEmail Help section](#) if you have any questions regarding this message or your MaxEmail service.

Thank you for using MaxEmail!



You have received this message because you are registered as a MaxEmail subscriber. If you have any questions regarding your MaxEmail service please visit www.maxemail.com.

[Signup for MaxEmail](#) | [Login to MaxEmail](#) | [Help](#)





A Public Service Agency

VEHICLE REGISTRATION RENEWAL NOTICE



VEHICLE REGISTRATION RENEWAL NOTICE

VIN	MAKE	YR	BODY TYPE	LICENSE PLATE	AMOUNT DUE	DUE DATE
1GNEK13T64R106036	CHEV	2004	UT	5CYE584	\$177	08/08/2010



SMOG Certification Required (See reverse side of notice).



Please take this notice to a **SMOG** check station.



To renew, just provide:



Renewal Fees



Evidence of Liability Insurance

(see reverse side of notice)



SMOG Certification

(see reverse side of notice)



Return by MAIL only

FEES

REGISTRATION FEE	\$56
LICENSE FEE (May be an income tax deduction)	\$111
WEIGHT FEE	\$0
SPECIAL PLATE FEE	\$0
COUNTY/DISTRICT FEES	\$10
OWNER RESPONSIBILITY FEE	\$0

TOTAL DUE ON OR BEFORE 08/08/2010 \$177

OR \$18 TO FILE PLANNED NONOPERATION

LATE PAYMENT

POSTMARKED	RENEWAL	PNO
After 08/08/10 through 08/18/10	\$208	\$39
After 08/18/10 through 09/07/10	\$229	\$55
After 09/07/10 through 11/06/10	\$304	\$115
AFTER 11/06/2010	\$304	NO PNO

PLANNED NONOPERATION

If you plan not to operate (PNO) this vehicle, please check the box and return the bottom part with your PNO payment.



DETACH AND RETURN

Planned Nonoperation

Change of Address (see back)

For DMV Use Only

☐
☐
☐

1
S

#0717

1221111A	B051110F01	02789	P10002
LICENSE NUMBER	MAKE		
5CYE584	CHEV		
VIN			
1GNEK13T64R106036			
DMV USE	DUE DATE	AMOUNT DUE	
	08/08/2010	\$177	

MAKE PAYMENT TO:

M7 RENTALS LLC
712 LINCOLN AVE
PO BOX 321
ALAMEDA CA 94501

DMV RENEWAL
P.O. BOX 942894
SACRAMENTO CA 94294-0894



020101051234140508040017700220000060001000005030600000000127001603699958

Fuller, Amber

From: Lindsey, Drennon
Sent: Friday, August 06, 2010 8:47 AM
To: Bang, Steven R.; Campbell, Rebecca A; Elder, Nicole; Glock, Bob; Gonzales, Patrick M.; Knight, Shawn; Lane, Cassandra; Lewis, Eric; Morrow Jr., Frank; Mosley, Pierre; Reed, Kevin; Shavies, Frederick; Thomas, Mark D; Trevino, Robert A.; Wingate, Randell
Subject: FW: Interview questions
Importance: High

In case you get a 459 call out.

From: Meeks, James
Sent: Thursday, August 05, 2010 1:17 PM
To: Biddle, Phyllis; Gall, Philip; Hicks, Mark; Jacobs, Adriane; Muniz, Robert; Rhee, Simon; Salcido, Daniel; Silva Rodriguez, Robert R.; Somarriba, Edwin
Cc: Tull, Steven; Lindsey, Drennon; Armstrong, Leronne
Subject: Interview questions
Importance: High

Effective immediately the following question shall be asked when interviewing burglary suspects:

- Why did you select this home or vehicle to burglarize?
- Do you live or have lived in the area?
- What types of loss do you prefer taking?
- Where do or who do you sell the loss items to?
- Why do you burglarize homes or vehicles in Oakland?
- If you are confronted by the home owner(s) are you prepared to defend yourself?
- Do you believe the DA's office will/or not charge you with first degree burglary?
- What do you need to turn your life around?
- What other crimes can tell us about?

These questions must be asked and written in your follow-ups. You are to research to see if the burglaries are happening in the major Hot Spot areas; by checking with the crime analysis. We must conduct a more in-depth interview of the suspects and why they are committing crimes in the City.

Lt. Meeks
Theft Section
jmeeks@oaklandnet.com
238-3951

Fuller, Amber

From: John Spomer <jspomer@penlink.com>
Sent: Friday, August 06, 2010 2:53 PM
To: Knight, Shawn
Subject: Maintenance Invoice
Attachments: Oakland Maintenance 10-11.xls

Hi Shawn,

Sorry to hear that your grant didn't go through.

In follow up to our conversation from yesterday, I have attached a maintenance renewal invoice for your LINCOLN System for the coming year (9/1/10 – 10/1/11).

Let me know if you have any questions.

John



John Spomer | Sr. Sales Executive
5936 VanDervoort Drive | Lincoln, NE 68516 | USA
402.421.8857 Office | 402.202.3500 Cell | 402.421.9287 Fax
jspomer@penlink.com | www.penlink.com

Learn about the 2010 Pen-Link CIA Conference at www.penlink.com/cia

CONFIDENTIALITY NOTICE: The information in this email is confidential proprietary property of Pen-Link, Ltd. Unauthorized use of this communication is strictly prohibited and may be unlawful. If you have received this communication in error, please immediately notify the sender by reply email and destroy all copies of the communication and any attachments.



It's the Key™

402.421.8857 Office | 402.421.9287 Fax

Bill To:

Oakland PD

Oakland, CA 94607

Same

Date:

8/6/2010

Invoice:

8062010

Tax ID:

Salesperson	Purchase Order	Ship Date	Ship Via	F.O.B Point	Terms
John Spomer					Net 30 after receipt of Purchase Order .

Quantity	Description	Unit Price	Total
1	LINCOLN MAINTENANCE BASED ON A 6-CHANNEL / 9-USER SYSTEM (9/1/10 - 8/31/11)	\$34,156	
			\$34,156
		Sub-total	\$34,156
		Tax rate	
		Sales tax	
		Shipping	
		TOTAL	\$34,156

Please remit to above address

Fuller, Amber

From: John Spomer <jspomer@penlink.com>
Sent: Friday, August 06, 2010 3:08 PM
To: Knight, Shawn
Subject: Pen-Proxy
Attachments: Pen-Proxy.doc; What's New Slick.pdf

Hi Shawn,

Included with this year's maintenance renewal is a new product called Pen-Proxy. Pen-Proxy adds the ability for Pen-Link v8 to communicate with various "outside" services including the FBI's i1020 national cell tower database and mapping precision location data from Sprint/Nextel, T-Mobile and AT&T Wireless.

Hopefully Pen-Proxy will give you more justification for renewing your maintenance. I've attached more information.

Have a great weekend.

John

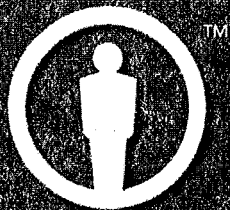


John Spomer | Sr. Sales Executive

5936 VanDervoort Drive | Lincoln, NE 68516 | USA
402.421.8857 Office | 402.202.3500 Cell | 402.421.9287 Fax
jspomer@penlink.com | www.penlink.com

Learn about the 2010 Pen-Link CIA Conference at www.penlink.com/cia

CONFIDENTIALITY NOTICE: The information in this email is confidential proprietary property of Pen-Link, Ltd. Unauthorized use of this communication is strictly prohibited and may be unlawful. If you have received this communication in error, please immediately notify the sender by reply email and destroy all copies of the communication and any attachments.



PEN·LINK™

It's the Key™

Pen-Proxy



Pen-Link, Ltd.
5936 VanDervoort Dr.
Lincoln, NE 68516

Phone: (402) 421-8857
FAX: (402) 421-9287

Revision 01
June 2, 2009

Pen-Link, Ltd. is a
U.S.-Based Small Business

DUNS: 195956636
TIN: 47-0707585
CAGE: 0K6H9

Contents

1.	Pen-Proxy	1
1.1	NeuStar LEAP Interface	1
1.1.1	Other Potential Data Sources.....	2
1.2	i1020 Cell Tower Database Interface	2
1.3	Real-Time Call Alerts.....	3
1.3.1	Alert Trigger Criteria	4
1.3.2	Methods of Alert Transmission or Notice	4
1.4	Precision Location Services	4
1.4.1	Email Delivery.....	5
1.4.2	Pen Register vs. Precision Location.....	5
1.4.3	Incorporation into Pen-Proxy.....	6



1. Pen-Proxy

Pen-Proxy is a new add on product for Pen-Link v8.1. Pen-Proxy adds the ability to Pen-Link v8.1, to communicate with various "outside" services, routing data to or from these services, thereby providing enhanced intelligence and capabilities to the Pen-Link end user. The functions scheduled to be included with Pen-Proxy upon its initial release are outlined in the following sections.



Pen-Proxy

1.1 NeuStar LEAP Interface

A basic requirement of working with telephone data is to match a subscriber with a phone number. To get a valid subscriber record, most people have to turn to the Telecommunications Service Providers (TSPs) themselves. This means knowing what TSPs service what phone numbers. Years ago, that wasn't a very difficult task. But since the national advent of Local Number Portability several years ago, intelligence analysts encounter ported phone numbers more and more frequently.

NEUSTAR®

NeuStar, the administrator for LNP throughout the North American Dialing Plan, made an Interactive Voice Response (IVR) system available to Law Enforcement Agencies (LEAs) some years ago. The system allowed LEA personnel to "look up" service provider information for ported numbers. But as valuable as the system is, it has its limitations:

- You have to access the system over the phone
- You can only look up a maximum of 20 phone numbers before the system disconnects
- The process was manual, and therefore time consuming.

Last year, in response to requests from LEAs, NeuStar implemented its LEAP system: the Local Number Portability Enhanced Analytical Platform. LEAP offers several advantages over the IVR system:

- LEAP is an online system, accessed through a VPN network connection or over a secure web connection
- LEAP lets you look up numbers in batches of 100 at a time
- The response is nearly real time
- The system works for **all** North American Numbers, not just ported numbers, providing OCN data and contact information for the TSP that services a phone number.

New/Update Phone Record	
Porting Information Porting History	
Phone Number	[402] 610 2347
Activate Date	[03/15/2008]
Ported	[Yes]
OCN	[6214]
Company Name	[CINGULAR WIRELESS, L2]
Contact Name	[SUPPORT]
Contact Phone	[800] 635 6040

[Save] [Cancel] [Help] [Print Record]

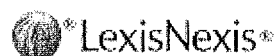
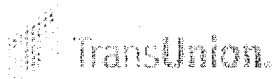
Working with the LEAP Services staff at NeuStar, we have recently developed an interface to the LEAP service directly through Pen-Link. The interface lets you:

- ➔ Do real-time queries, one phone number at a time
- ➔ Do batch lookups through the Pen-Lookup utility, with no upper limit on the number of phone numbers in the query (Pen-Link automatically takes care of the 100-number limit, automatically breaking your query into multiple queries, as required, if you have more than 100 numbers).

1.1 Third-Party Data Provider Interfaces

We are currently in discussions with other third-party data providers to develop interfaces between Pen-Link systems and various data sources that are used by our customers. Because development is still in process, we have mutual Non-Disclosure Agreements in place with these providers. As such, we are restricted from providing much detail. We can tell you that some of the data providers we're working with include:

➔ **LexisNexis**



➔ **LocatePLUS**

➔ **Trans Union (iQ411)**



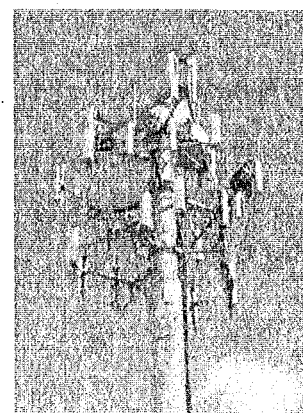
➔ **TARGUSinfo**

➔ Others that we are not at liberty to divulge at this time.

We are excited about these projects, and hope to have interfaces for these providers incorporated into Pen-Link Proxy in the very near future. Longer term, we envision incorporating even more interfaces to various providers of public records data.

1.2 1020 Cell Tower Database Interface

When working with call data from a wireless Target, a common analytical requirement is to find out what Cell Sites and Sectors the Target occupied during its calls. But U.S. Carriers do not typically provide actual locations, where for real-time Pen Register data or historical Call Detail Records (CRDs). Instead, carriers provide location codes—like L:3300 C:1036—that indicate which of their towers handled the call, and which face of the tower picked up the signal from the Target. These codes must then be compared to a separate database or other data set to find an actual location (e.g., latitude and longitude) for the tower, as well as the tower's orientation, effective range, etc.



Any analyst who has ever performed a location analysis on a wireless Target knows that there are often challenges to overcome for the analysis to be accurate.

- ➔ Cellular Carriers sometimes renumber their towers, often with no apparent rhyme or reason. This means that the tower that was designated "tower 3300" last month, may not be the same tower that's designated "tower 3300" this month.
- ➔ The original sources of cell tower location data are the Cellular Carriers themselves. Sometimes they don't easily "give up" the cell tower data. When they do, it will be delivered to you in various

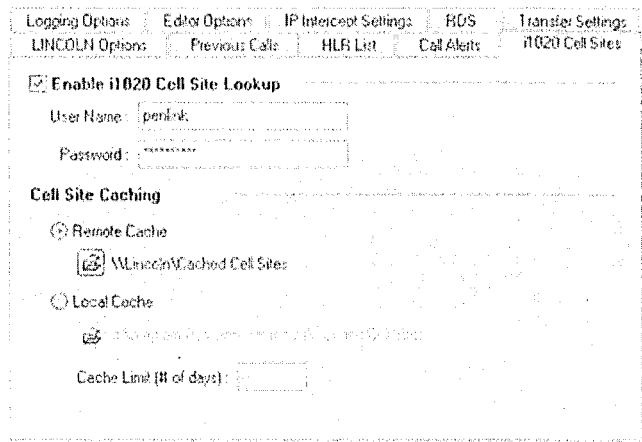
forms: .xls file, .doc file, .txt file, .csv file. As with Toll Records, no carrier's data file format is like another's! Some may even provide the cell tower data on paper!

For a location analysis of a wireless Target to be meaningful, the data in the cell tower database must be recent and available in a timely manner. Recognizing the challenges, the U.S. Department of Justice, through it's AskCALEA organization, has developed a secure on-line database called the i1020 Cell Tower Database. The i1020 database contains the most recent cell tower location data for most U.S. Cellular Carriers. When queried with a location code typically found in call transaction data, the system identifies the corresponding tower and sector, and returns the following information:

- ➔ Latitude (of the tower, in decimal format)
- ➔ Longitude
- ➔ Azimuth (orientation of the tower face, in degrees)
- ➔ Beam Width (e.g., 120 degrees)
- ➔ Effective radius (e.g., 1.86 miles)

This database can be accessed over a secure web connection. The system also provides an API (Application Programming Interface) that will allow third-party software to connect to it over a secure VPN connection. Hey! We're a third-party software manufacturer! So guess what we've done? We've developed an interface from Pen-Link to the i1020 Cell Tower Database! This interface will:

- ➔ Look up the cell tower and sector locations for a Target—in real time—as you collect live call data for a Pen Register or a Title III intercept.
- ➔ Look up cell tower and sector locations from Pen-Link reports.



The i1020 Cell Tower Database is operated by the DOJ's AskCALEA organization. LEAs can apply for access through AskCALEA. For more information about the network requirements and the application process, please contact the i1020 Team at i1020@askcalea.net.

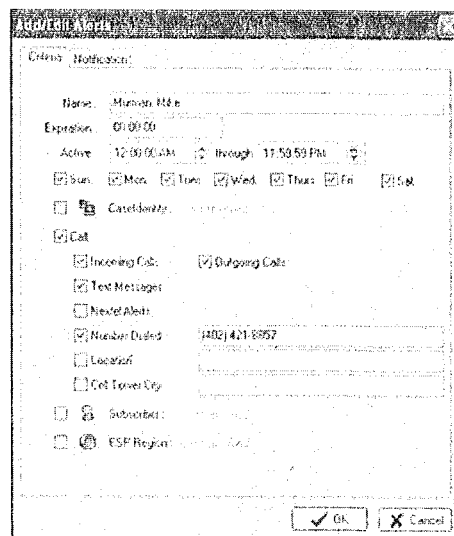
1.3 Real-Time Call Alerts

Customers have asked... now they shall receive. Receive call alerts, that is! Pen-Link users who conduct Pen Register and Title III intercepts have recently asked us to incorporate automated, real-time call alerts into the system. So we have!

With the Real-Time Call Alert service of Pen-Link Proxy, you can define a wide variety of alert trigger circumstances and methods of alert transmission. You could, for example, have Pen-Link send you an email alert every time one of your Targets receives a Text Message during the weekend. Or have Pen-Link send you a text message alert when one of your wireless Targets is in or near one or more specified cell tower locations. The system allows a wide variety of flexibility in defining the criteria that will trigger the sending an alert via email or SMS.

Alerts and Notifications

- ➔ Specific Case Identity
- ➔ Various Call Fields
 - Direction - alert for incoming, outgoing, or both
 - Presence of a Text Message
 - Presence of a Nextel Alert
 - Presence of Specified Numbers Dialed
- ➔ Location
 - Specific LAC/CID pairs
 - Or open to any valid location in messaging
- ➔ Cell Tower City (based on the Cell Tower database)
- ➔ Matched to Specified Subscriber Records
- ➔ Wireless Target activity overlapping defined Electronic Surveillance Perimeters ("Geofencing")



Wireless Alerts and Notifications

- ➔ Defined alerts attached to Case IDs
- ➔ When conditions are met for a defined alert, one or more of the following types of alerts are triggered:
 - Audio Alert - Play a user-selected .wav file
 - SMS Alert - Send a text message to one or more cell phone through an Email-to-SMS Gateway
 - Email Alert - Send an email message directly to one or more email accounts

Need to know what your intercept Targets are doing, but can't watch the Pen-Link Intercept Screen all day? The new Pen-Link Automated, Real-Time Alerts are your key!

4. Precision Location Services

Some wireless telephone service providers now make another real-time surveillance service available to Law Enforcement. Known by several different names (e.g., "Mobile Locator Results"), these services rely on the same E911 infrastructure that a carrier would use to deliver real-time location information for wireless phones to 911 emergency call centers. But instead of delivering the data to a call center, the carrier delivers the data to the requesting Law Enforcement Agency. As with E911, the data delivered is meant primarily to indicate the location of the target phone.



Unlike a pen register, these Precision Location services do not deliver transactional call detail data, such as the direction of a call, the duration of a call, the number dialed, etc. The Precision Location data includes a Date/Time stamp and a Lat/Long pair. Some providers may provide additional information, such as an estimated degree of accuracy, given as the radius of a circle centered on the reported Lat/Long (some providers call it "certainty," some call it "uncertainty"... it's an estimate of possible error).

4.1 Email Delivery

When implemented for Law Enforcement, Precision Location delivery services typically deliver the data in plain text using simple email delivery. The receiving agency designates an email address for the carrier to send to. The emails arrive periodically. As you might expect, different carriers format the emails different ways; the example below shows the formatting currently used by AT&T.

From: AT&T Mobility Compliance (No Reply) [mailto:noreply@att.com]
Sent: Wednesday, February 04, 2009 8:32 PM
To: undisclosed-recipients
Subject: Mobile Locator Results for 530026

AT&T PROPRIETARY Solely for authorized persons having a need-to-know
pursuant to Company instructions
AT&T CONFIDENTIAL - DO NOT FORWARD.
Initiated 2009/2/4 20:32:45

The mobile number was located on Wed Feb 04 22:03:55 CST 2009.

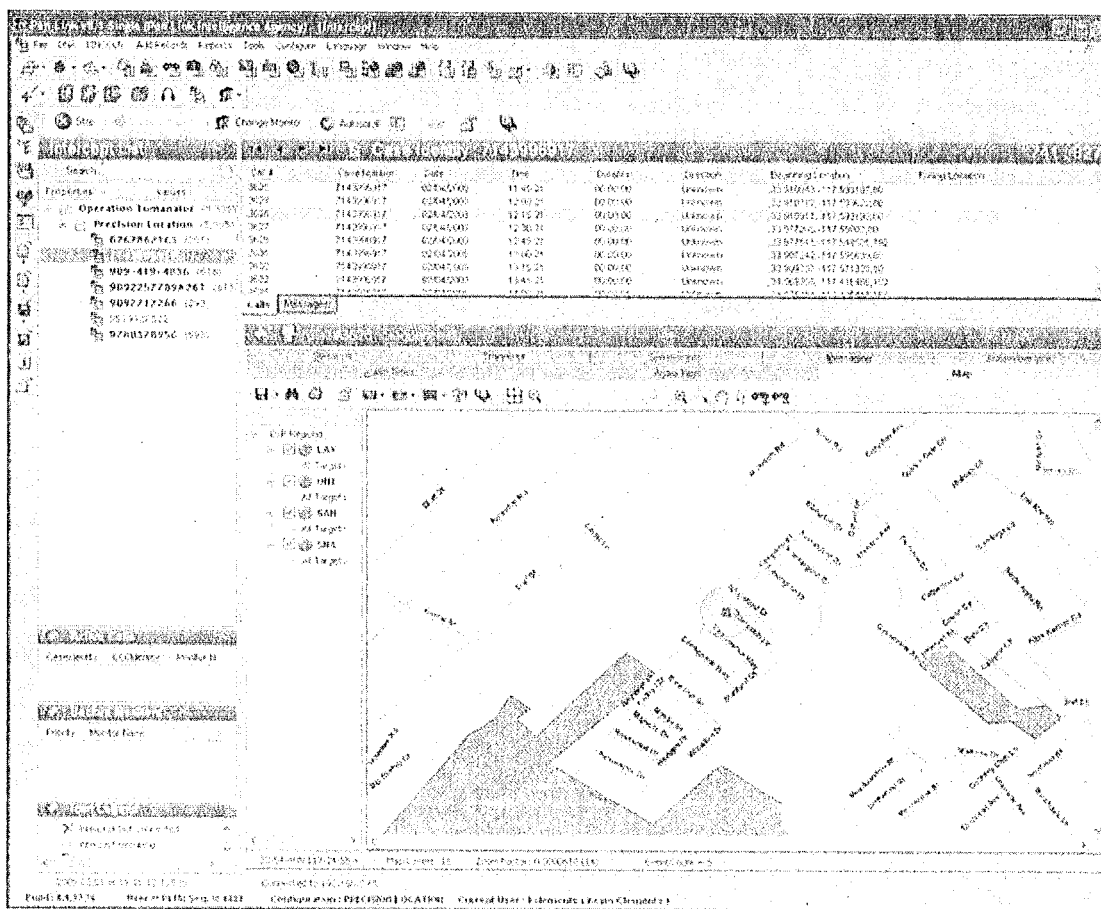
ITN	530026
Case_ID	
Mobile Number	
Result ID	Updated
Source	SMILC
Confidence	Varied - System unable to determine technology
Cell Location	Unavailable
Longitude	-117.58301 degrees
Latitude	34.10483 degrees
Altitude	Unavailable
Altitude Certainty	Unavailable
Elliptical Resolution	
Minor Axis	1,057 metres (Certainty Factor)

Because they provide no transactional data, these services would be of less use in some circumstances than in others. For example, such a service is of little use in developing a target phone number for a fugitive whose phone number is unknown at the start of the case; traditional pen register and toll data from the phones of family, friends and other associates would be more effective in this regard. But once a fugitive's phone number is known, if all that is desired is location data for that phone, then a Precision Location delivery service, if available from the target's carrier, will provide more accurate location information than the cell tower and sector data normally found in J-STD-025 messaging for a pen register

on a wireless target. Not only would the location data be more accurate, but in our experience, the fees for these Precision Location delivery services tend to be much lower than the usual fees for provisioning pen registers.

4.2 Introduction to Pen-Proxy

We have taken the approach that it should not matter whether you are collecting live pen data or live Precision Location data for any given target; both should come into the same interface and end up in the same analytical database. To this end, we have include Precision Location collection as part of the new Pen-Proxy services. Incoming emails containing the location data are received by the Pen-Proxy Server. As the emails arrive in real time, the data—no matter the original text format—is extracted from the email, parsed into logical fields, mapped to corresponding Pen-Link fields, and loaded into the Pen-Link database as Call Records (so that they may easily be mingled with analysis of your other call data). The delivered Lat/Long and reliability (error) information is then immediately available to the agent or analyst in the field in the live Pen-Link collection window (as shown below) or through Pen-Link reports. With Pen-Link's GIS Mapping option, the Lat/Long coordinates, along with the "certainty" estimate are automatically plotted in the Map tab of the live collection screen.

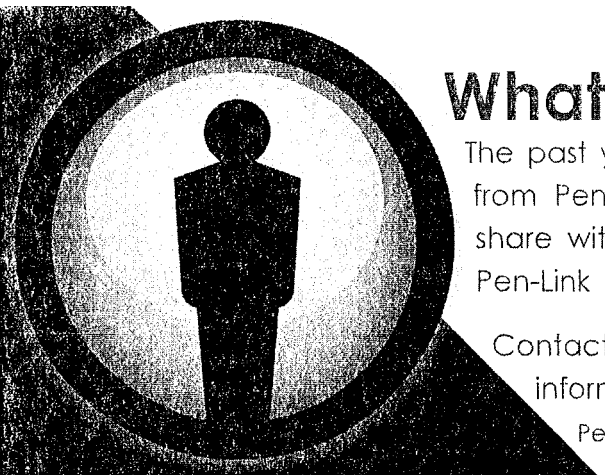


To our knowledge, there are only three wireless carriers currently offering this type of surveillance service:

- ➔ AT&T
- ➔ Sprint/Nextel

➔ T-Mobile.

We have incorporated all three delivery formats into Pen-Proxy. As has always been our practice, we will continue to incorporate changed or new formats as they come along.



What's New?

The past year has seen several exciting new technological developments from Pen-Link, Ltd. As a result, we have several great new features to share with you! Keep reading to learn more about the new features in Pen-Link and how our new developments can make your job easier.

Contact us at 402.421.8857 or sales@penlink.com for more information and to get started with everything new at Pen-Link.

Pen-Link, Ltd. 5936 VanDervoort Drive Lincoln, NE 68516

Pen-Proxy

Pen-Proxy lets Pen-Link v8.1 and LINCOLN v2.1 communicate with various "outside" services, routing data to or from these services, providing you with enhanced intelligence and capabilities directly from within Pen-Link.

Tracking down ported phone numbers? No problem. Pen-Proxy's **NeuStar LEAP Interface** lets you:

- Do real-time queries, one phone number at a time
- Do batch lookups through the Pen-Lookup utility, with no upper limit on the number of phone numbers in the query (Pen-Link takes care of the 100-number limit)

We are currently working with other third-party data providers to develop interfaces between Pen-Link systems and various other data sources used by our customers.

NEUSTAR®

TransUnion
TARGUSinfo

LOCATE

Need cell tower locations? Pen-Proxy's **i1020 Cell Tower Database Interface** will:

- Look up the cell tower and sector locations for a Target — in real time — as you collect live call data for a Pen Register or a Title III intercept.
- Look up cell tower and sector locations from Pen-Link reports.

Information available for cell towers includes latitude, longitude, azimuth, beam width, and effective radius.

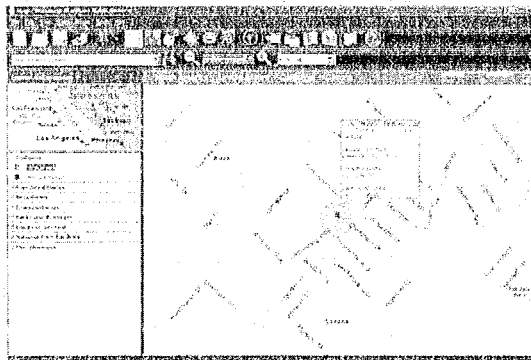
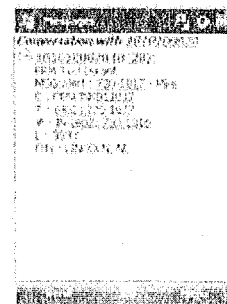
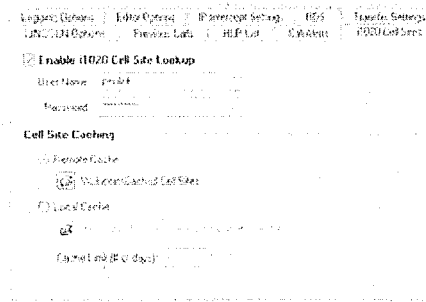
Need to know what your intercept Targets are doing, but can't watch the Pen-Link Intercept Screen all day? With Pen-Proxy's **Real-Time Call Alerts**, you can define a

wide variety of alert trigger criteria and methods of alert transmission including:

- Audio Alert - Play a user-selected .wav file
- SMS Alert - Send text messages to cell phones through an Email-to-SMS Gateway
- Email Alert - Send email messages directly to one or more email accounts

Looking for more location data for a Target's phone? Pen-Proxy's **Precision Location**

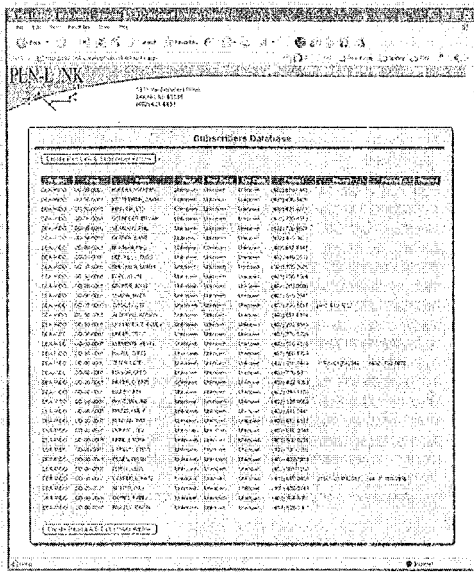
Services interfaces with carriers' Email Ping delivery systems, providing more than the cell site and sector information typically found in Pen Register data. With Precision location service, you'll get electronic delivery of data at regular intervals, including a Date and Time, the Latitude and Longitude of the phone, and a degree of certainty measure, which Pen-Link plots, in real time, as the radius from the given Lat/Long center. This type of service is currently offered by Sprint/Nextel, AT&T, and T-Mobile, and Pen-Proxy supports all of their delivery formats.



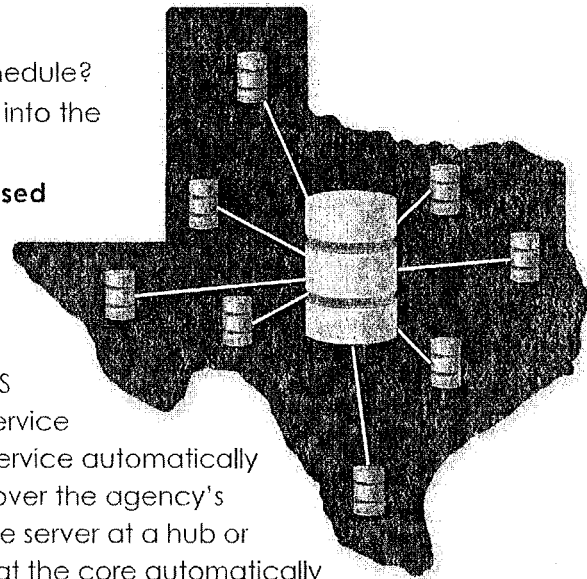
Pen-Link Automated Mirroring System (PAMS)

Have you ever wanted to:

- Export Pen-Link data from multiple sites to one **central intelligence database**?
- A central **SQL** database?
- Export manually, whenever you want?
- Or have Pen-Link **export automatically**, on a time-based schedule?
- Have the system **automatically upload and import** the data into the central database?
- Access the central database through an easy, fast, **web-based thin client**?



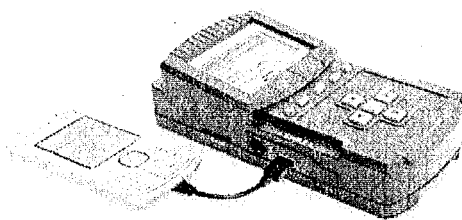
The new **Pen-Link Automated Mirroring System (PAMS)**, now makes all of this possible. PAMS incorporates an automated service that runs at remote sites. This service automatically "pushes" database changes over the agency's network, to a central database server at a hub or "core" facility. Other services at the core automatically load the pushed data into a Pen-Link v8.1 Master Database or an SQL-based **Pen-Link SQi** Master Database. In this way, the Master Database at the core mirrors all of the operational databases in the field. **Pen-Link SQi** also offers a browser-based **Thin Client** for field users to query the SQi Master Database and optionally bring data back to the field for additional analysis in Pen-Link v8.1.



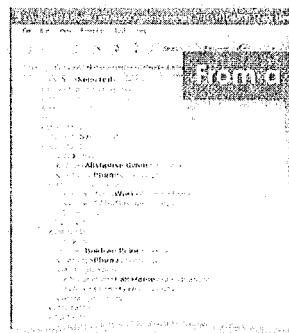
Cell Phone Forensics

Want to do more with the data you extract from cell phones? Autoload it! Pen-Link v8.1 now offers a Cell Phone Forensics feature that can Autoload the files produced by forensic cell phone data extraction systems. Unlike traditional Autoloading of Toll, CDR, or Subscriber data from phone companies, when you Autoload a cell phone forensic file, Pen-Link populates multiple database simultaneously. The phone's Call History would load as Call Records; the Contacts List would load as Subscriber Records; Multimedia (images, videos, ringtones) would load as Event Records. Once you have the data from multiple phones loaded into Pen-Link, you can bring Pen-Link's reporting and analysis capabilities to bear. You could, for example, use Pen-Link's built-in Common Subscribers by Case report to easily identify contacts that are common across multiple seized phones.

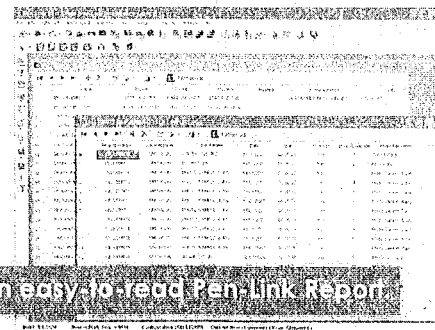
CelleBrite
Universal Forensic Products



Pen-Link's Cell Phone Forensics function currently supports Cellebrite's popular Universal Forensic Extraction Device (UFED). Support for other devices may be added in the future.



From a hard-to-read xml file



To an easy-to-read Pen-Link Report

Fuller, Amber

From: Jaecksch, Julie
Sent: Wednesday, August 11, 2010 5:57 AM
To: Allison, Michelle R; Ann Pierce; Ausmus, Lisa L; Backman, Ray; Barry Hofmann; Bryan Hubbard; Campbell, Rebecca A; Chuck Ilacqua; D'Aloisio, Kasi N.; Dan Kemmitt; Daniel Royal; Darrin Downum; Davina Kelly; Don Sawyer; Doria Neff; Downing, David; Downum, Darrin; Gonzales, Patrick M.; Hofmann, Barry; Hubbard, Bryan; Irma Grieve; Jaecksch, Julie; Jayson Landeza; Jeff Hassna; Joe Quintela; John Muschi; Julie Derby Jaecksch; Kasi D'Aloisio; Kelly, Davina; Kemmitt, Daniel P.; Knight, Shawn; Lee, Mega; Levine, Melonie; Lindsay Lyons; Lisa Ausmus; Lozares, Demetrio; Lyons, Lindsay; Maggie Dorsey; Mahanay, Patrick; Maria Sanchez; Mega Lee; Melonie Levine; Michael Palmertree; Michelle Allison; Moore, Robert L; Muschi, John P; Neff, Doria; Parris, Kenneth; Pat Gonzales; Pat Mahanay; Pierce, Ann M.; Poulson, Edward; Quintela, Joe C; Rachael Van Sloten; Renee Hassna; Rob Roche; Robert Moore; Roche, Robert R.; Royal, Daniel A; Sanchez, Maria S.; Sawyer, Donald; Shawn Knight; Steve Szopinski; Szopinski, Steven B; Taylor, Yanicka; Topacio, Patricia; Van Sloten, Rachael; Yanicka Taylor
Subject: peer support
Attachments: Team Meeting 28JUL10.wps.rtf

hello everyone -

i have attached the notes from the team meeting that was held on july 28th.

i want to thank those team members who have given me their current work assignment and contact information for the team listing on the protected area of the improved Departmental intranet which should be online soon. if you think that i might not have your current information and/or if you have recently changed assignments due to the reorganization, please email me. our co-workers who are looking for guidance and the commanders who are making a call-out must be able to locate accurate & complete information for our team members. thank you for your cooperation.

thanks for being a member of the team.

take care and be safe.

julie



PEER SUPPORT TEAM MEETING
JULY 28th 2010

WE ARE NOW 41 MEMBERS STRONG !!

34 CURRENT OPD

1 MENTAL HEALTH PROFESSIONAL

RENEE

3 RETIRED OPD

2 CHAPLAINS

INTRODUCTION OF ALL TEAM MEMBERS AT THE MEETING

Michael Palmertree asked me to say that he is sorry that he could not be here today but he and his wife had an appointment that could not be changed.

PRESENTATION BY LT. BRIAN MEDEIROS OF THE HOMICIDE UNIT:

WHAT PEERS CAN TELL INVOLVED OFFICERS ABOUT THE INVESTIGATIVE PROCESS
TO EASE THEIR MINDS & PREPARE THEM FOR WHAT WILL HAPPEN

Brian started his discussion at the scene immediately after a critical incident:

-The Homicide Unit investigates all Officer-involved shootings except accidental discharges where no one is injured.

-As soon as Homicide is called, they have the lawyer(s) from LDF called to respond to minimize the waiting times.

-The involved Officer(s) (involved in a shooting most commonly) must be sequestered and must have someone that they are comfortable with stay with them at all times.

-When there are multiple involved Officers, they must be kept separated so they are not talking about the incident and so no one can perceive that happened.

-The Officer(s) does a walk-through at the scene with the Homicide Investigators and gives a brief public-safety statement so that evidence can be located and suspect(s) can be found. The Officer may not do this if there is a hostile crowd and/or the incident is captured on surveillance video that can be viewed immediately. If there is going to be a long delay in the response of the Homicide Investigators, the scene supervisor may be given permission by Homicide to allow the Officer(s) to leave the scene prior to the arrival of the Homicide Investigators. The Officer(s) would then return to the scene for the walk-through

and public safety statement. Having involved Officer(s) leave the scene should be avoided whenever possible.

-Photographs of the Officer(s) may be taken at the scene as soon as the scene is secure, especially if their uniform became disheveled and/or dirty during the incident.

-The Officer(s) goes to the PAB. It is OK for the Officer(s) to get something to eat and drink. It is OK for the Officer(s) to call his/her significant other or family to say that he/she is OK. Maggie Dorsey asked if there is anything in place for the significant other and family of the Officer(s) and Brian said that there is no official process in place but that each Officer is encouraged to tell their significant other/family what to expect from the media and about the process of the investigation. Robert Moore asked if it is OK if Peers ask the involved Officer(s) if they want the Peers to make any calls on their behalf and Brian said that this would be fine.

-The Officer(s) will be photographed and his/her weapon(s) & magazines will be taken. Homicide has loaner guns available. The Technician or Investigator will count the live rounds remaining in the pistol & magazines. The pistol will be examined and tested by an OPD Rangemaster and by one of the OPD ballistic experts before the pistol can be returned to the Officer.

-The Officer may change into civilian clothes after the photographs have been taken and get as comfortable as possible and try to relax.

-The Officer can wait with his/her friend and the Peer(s) in the CID Captain's office until the LDF attorney arrives. Then they will all wait for the investigators to be ready for the Officer(s). When there are multiple involved Officer(s), other locations will be used as well.

-Homicide Investigators really try to interview the Officer(s) within 3 hours. When multiple Officers have shot, they attempt to expedite the interviews by calling in additional Investigators.

-The interview will take place in the Captain's office. Officers are not placed in the same interview rooms that are used for suspects. The two Homicide Investigators and the Homicide Lt. will conduct the interview. If there is a fatality, a DA & DA Inspector will also be involved with the interview. The Investigators will use a written list of standard questions including: the basic information before the event; the event; & all of the event details so that no second interview is necessary.

- The Officer(s) will be asked who they called after the incident.
- IA Investigators and monitors can listen to the interview from another room via speaker phone but they cannot ask questions unless they ask the Homicide Investigators to ask the question in advance. By the rules of the NSA, the IA Investigators and the monitors have full access to the Homicide case file.
- The involved Officer(s) is given information on how to contact Michael Palmertree or another mental health professional who they must see before returning to work. The involved Officer(s) is given a minimum of 3 regular working days off and more can be arranged if desired. It will up to the Officer's Lt. to list the extra days off as administrative leave or sick leave.
- A question was asked about why the statements are taken so quickly after the incident and Brian said that the investigators want the incident fresh in the Officer's memory and that they do not want to delay the interview because there may be a perception that during that time the Officer(s) got his/her story straight or talked to other people.
- Other types of incidents such as in-custody deaths and crashes following a pursuit that result in injuries or deaths are treated essentially the same as an OIS incident. The Investigators use the same standard questions and the process is the same. Homicide also investigates every Level 1 use of force with an intentional strike to the head even if the person struck is going to be fine, 1-2 a year.
- I asked Brian to explain why Officers are no longer able to wait at the OPOA until the investigators are ready for them. He said that it is to avoid the perception that Officers are "getting their stories straight" while no one is watching them. The investigators do not think this but it could be the perception of the monitors, the media and/or the public.
- Homicide Investigators appreciate that Peers respond. Peers should stop the Officer(s) if he/she begins to talk about the facts of the incident. They know that it is helpful for the Officer(s) to be told about what types of reactions and feelings they may experience in the days and weeks after the incident as well as preparing them for what the process of the investigation entails. Brian thinks that it is a good idea for the Peers to wait until the Officer is done with his/her interview to touch base with the Officer and perhaps offer him/her a ride home.

CRITICAL INCIDENTS SINCE OUR LAST MEETING

****27MARCH**, OIS, at OPD transportation, shooters–Gary Foppiano & Jeff Loman, approximately 16 witness officers, 1 Technician (Middleton) and 2 Dispatchers (#73 Blanca beginning and then #63 Lydia). Peers were called out (Pierce & Roche). Michael Palmertree was out of town so the involved Officers saw Mike Smith separately, a group CISD was set-up for the others on 06APR but no one showed up. Possible reasons – only shooters/involved Officers are **required** to meet with mental health and the delay in the meeting. One of the peers suggested that the involved Officers might not have been able to get the attention they needed with such a large group if the witness Officers had come to a CISD. I reached out to the Dispatchers. While we try to encourage people to participate in the group debriefing process which has been shown to be beneficial, the choice is up to each involved Officer if they want to participate in a group CISD or have a private session with a mental health professional.

****22APRIL**, OIS, non-fatal, on day shift, Victor Garcia and witness Officer Nancy Cerecedes, on-duty Peers utilized and Victor met with Michael.

****17JULY**, OIS, fatal, 3 OPD shooters and 2 BART shooters. Peers were called out (Campbell, Knight & Taylor). A group CISD was recommended, one of the shooters was not available so he went to see Michael individually. Michael told me that the Peers did an excellent job and that this case illustrates how important and beneficial it is to have Officers with OIS experience as part of the Team.

Robert Moore was contacted by BART. We discussed that multiple agency OIS incidents can be complicated and they seem to be happening more often lately.

****26JULY** peers were called-out to assist Officers who were being questioned by Homicide and IA investigators about the death of a man while the Officers were on scene at an incident on the morning of 22JULY. This was being treated similarly to an in-custody death even though the Officers had not touched the man. One of the on-call peers could not be reached. I made multiple calls to find a second person to respond. This is an example of the possibility of getting a call when you are not on-call but if you are not available that is OK. I try to see if anyone is on-duty, going in for a shift soon, lives close, etc. It is not a good idea to send only one peer to a call-out.

****Any others ?** *none that people present knew about.*

We talked about the turmoil of the pending layoffs, contract negotiations, anger, fear and stress going around the Department.

IMPROVED OPD INTRANET

The handout with team members information is what I have already submitted to be placed on the password-protected portion of the site. If you want me to make any changes let me know ASAP. This is an important step for the team. Any OPD employee, Supervisor or Commander with access to a computer will be able to bring up the list of team members and their contact information as well as the call-out calendar. This is another reason why I need to have current information about all team members.

MEETING WITH CHIEF BATTS THAT OCCURRED 28APRIL2010

- His support of the Team.
- He requested the recruitment of additional team members.
- Michael and I told him about our vetting of local mental health professionals so that we can make the best referrals.
- I prepared this chart (taped to the wall) in response to Chief Batts wanting to know how our Peer Support program compares with other agencies and we are doing very well.
- We need to become more vigilant about completing the monthly contacts page to track the utilization of the program. I have a form that I can email to each of you every month to be completed and returned.

TRAINING OPPORTUNITIES

**SEPT in SF – they are holding 4 spots for OPD so please let me know if you can go to this class Knight, *Gonzales & Roche will go.*

**OCT in San Ramon – I know this instructor very well

SUICIDE PREVENTION TRAINING and BOOKLETS

--The training continues during Officer CPT and sessions targeting Sgts. have been held. Other sessions targeting the rest of OPD personnel will be held in the near future I hope.

--Does anyone not have a copy of the Suicide Prevention booklet? *I distributed booklets to new team members.*

Maggie Dorsey brought up that last week she was made aware of a law

enforcement suicide that had been a client at WCPR. Her point was that sometimes even after help is provided, the person needs ongoing care and watching and that we must get anyone who is suicidal whatever help they need whenever they need it.

UPCOMING EVENT

--OFD Light Of Lights SEPT. 15th 6:30

IMPORTANT REMINDERS

PLEASE KNOW WHEN YOU ARE ON-CALL. If something comes up--find a replacement and let me know.

WHEN YOU RESPOND TO A CALL-OUT you need to email information about the incident to Michael, Renee and me - HANDOUT.

OUR HIGHER PROFILE MEANS PEOPLE ARE WATCHING INCLUDING CHIEF BATTS.

Chief Batts has expressed his definite support for the peer support program.

With this increase in expectations comes an increase in responsibility. We MUST answer the calls for assistance and fulfill the requests that we are given to maintain our credibility as a group that can be counted on. In June DC Israel asked for a DL-email about the Peer Support Team and the EAP programs because of all the stress of the potential layoffs and reorganization, etc.

VETERANS & RESERVISTS

Dave Downing is the OPD Veterans Affairs Officer so refer people who need information about benefits and other topics related to military service to him.

BROCHURE

--Renee did a great job with the updated brochure which we will get printed as soon as we add the newest team members.

I NEED UPDATES WHEN YOUR WORK ASSIGNMENT CHANGES, DAYS, HOURS, LOCATION, ANY PHONE NUMBERS OR EMAILS PLEASE

OLD BUSINESS

A question was asked recently if involved Officers could wait at the OPOA until the

Investigators were ready to interview them like the way it was done in the past. I asked Michael and he told me that Chief Batts had recently been asked to reconsider the current policy of having Officers wait at the PAB. Chief Batts said that the procedure will stay as it is based on his experience in Long Beach and the perception that the monitors have that waiting at the OPOA allows Officers to "get their stories straight".

NEW BUSINESS

Renee gave me a new phone number for MHN – the 24/7/365 number has been changed. I sent a DL email and I changed it for the intranet. As well as emailing the team

HANDOUTS

- *Team members contact information

- *Call-out procedures

- *MHN mental health professionals with experience working with law enforcement personnel and their families

- **Article from the Contra Costa Times about the West Coast Post-Trauma Retreat.

- **Article from Law Enforcement Technology "Surviving Law Enforcement".

- **3 MHN flyers.

- **Measuring Life Stress

- **Suicide articles: Australia; Army; Kate Scannell-"Suicide: a Deadly Social Burden".

- **PTSD symptoms

ATTENDED: Campbell, D'Aloisio, Dorsey, Gonzales, Grieve, Renee Hassna, Ilacqua, Jaecksch, Kelly, Kemmitt, Knight, Levine, Lyons, Mahanay, Moore, Neff, Royal, Sawyer and Topacio.

KNOWN ABSENCES: Downum, Landeza, Palmertree, Van Sloten.

I distributed handouts to all team members not at the meeting including asking them to update their information to me for the OPD intranet.

Julie Derby Jaecksch

28JULY10

Fuller, Amber

From: Joshi, Nishant
Sent: Monday, August 16, 2010 10:51 AM
To: Knight, Shawn
Subject: Cost analysis for stingray

Shawn

The Captain is doing his CID budget today. He needs to know how much the stingray costs annually. Please let me know by today. Otherwise he will do his budget without including the stingray. If that happens, we will start using other federal agencies for the stingray.

Fuller, Amber

From: Alex Nocon <Alex.Nocon@doj.ca.gov>
Sent: Thursday, August 19, 2010 7:04 PM
Subject: Fwd: FW: Telephone Investigations Resource Guide With POCs
Attachments: Telephone Investigations ResourceGuide .2010.pdf

>>> Karen Sherwood 8/19/2010 5:45 PM >>>

Telephone Resource Guide attached. Good info/contact tool to keep in your tool box!!

Karen

CONFIDENTIALITY NOTICE: This communication with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication.



STEP 1 - Determine the target phone service provider:

- **NeuStar**
(NPAC) **Number Portability Administration Center** <http://www.npac.com/lawenforcement/registration.shtml>
- CODE#** XXXXXXXXXXXX - obtain your own PIN from NeuStar by registering at the link listed above
- Automated Number** (571) 434-5781 NeuStar HELP Line (571) 434-5395

NOTE: If you query a number through NeuStar and it has "NOT BEEN PORTED", check it through Fone Finder to determine the likely service provider.

- **Fone Finder** <http://www.fonefinder.net/>

TIP: To identify providers for "800" numbers, call (888) 767-3300 Option 1

STEP 2 – Determine if the case involves - “Exigent Circumstances” (e.g. Abduction, Missing Person at risk or Dangerous Fugitive)

If so, using the provider resource list, contact the provider and tell them: *"We are investigating a case that we believe is an emergency involving immediate danger of death or serious bodily injury."* Do not explain the situation in detail - as they only need to have a *reasonable belief* that the situation involves immediate danger of death or serious injury. The provider will typically verify your information and then send you their Exigent Circumstance Request form via fax. A few providers require you to send your request via fax on official letterhead. Complete the form or the letter and fax it back. Some providers will require a valid Court Order to be submitted within 48 hours of the Exigent Circumstance Request.

TTP: If the target phone is roaming on another provider's network – complete the Exigent Circumstances process with the roaming provider to get the best and fastest results for call records and tower locations.

STEP 3 – Determine needed records & legal process required:

NOTE: Before submitting Subpoenas, Court Orders or Search Warrants, it is a good idea to contact the provider identified through the steps listed above and confirm that they are indeed the provider for the account. It is also recommended that you verify the provider's legal compliance process and contact information to avoid any delays or confusion.






- **PRESERVATION LETTER:** A preservation letter [USC 2703(b) (2)] should be sent to the provider via fax as soon as possible to preserve records before they are discarded and cannot be recovered. This is particularly an issue with text message and voice mail content which are generally only retained for 72 hours. *A sample preservation letter is included on the last page of this guide.*
- **SUBPOENA:** For basic transactional records (e.g. Subscriber account details, Billing Records or Account Notes) only a Subpoena is required. Submit the Subpoena via fax to the provider's Subpoena Compliance fax number. **Call the provider to verify receipt!**
- **COURT ORDER:** For detailed records (e.g. In-coming & Out-going Call Detail, Cell Tower Locations – including location “pings”, Text Message content, Voice Mail content and PEN Registers) a Court Order (or Search Warrant) is required. Submit the Court Order (or Search Warrant) via fax to the provider's Legal Compliance fax number. It is also a good idea to include a cover letter that includes your contact information, the target number and the specific records you are requesting and specify that you would like the records returned in an electronic format (e.g. Excel). **Call the provider to verify receipt!**



LAW ENFORCEMENT TELEPHONE INVESTIGATIONS RESOURCE GUIDE

– Cellular, Satellite & VoIP Phone Providers













 AT&T Mobility (Cingular) National Subpoena Compliance Center P.O. Box 24679 West Palm Beach, FL 33416 (800) 635-6840 Main (888) 938-4715 Fax <u>Physical Address:</u> 11760 US Highway 1, North Palm Beach, FL 33408	GSM	MVNO prepaid service as GoPhone Send a Text Message: AT&T Mobility [10-digit phone number]@txt.att.net Example: 2125551212@txt.att.net AT&T optional GPS location service: Family Map https://familymap.wireless.att.com/finder-att-family/welcome.htm
 Cricket Communications Subpoena Compliance 10307 Pacific Center Court San Diego, CA 92121 (858) 882-9301 Main (858) 882-9237 Fax	CDMA	Roaming partner with MetroPCS
 EMBARQ Law Enforcement Support 5454 W. 110th Street MS: KSOPK10402 Overland Park, KS 66211 (877) 451-1980 Main (913) 254-5800 Fax	CDMA	Embarq is the land-line division of Sprint / Nextel .
 OnStar ATTN: Records Request P.O. Box 430627 Pontiac, MI 48343 (888) 466-7827 or (248) 577-7465	CDMA	OnStar will need the registered user name, OnStar phone number or VIN. OnStar has an Emergency shut-down feature OnStar is an MVNO partner with Verizon
 MetroPCS Subpoena Compliance 8144 Walnut Hill Lane Dallas, TX 75231 (800) 571-1265 Main (972) 860-2635 Fax	CDMA	Send a Text Message: MetroPCS [10-digit phone number]@metropcs.com Example: 2125551212@metropcs.com



LAW ENFORCEMENT TELEPHONE INVESTIGATIONS RESOURCE GUIDE

– Cellular, Satellite & VoIP Phone Providers










<p>Qwest Communications Subpoena Compliance 1005 17th Street, Suite 120 Denver, CO 80202 (303) 896-2522 Main (303) 896-4474 Fax</p> 	<p>CDMA</p>	<p>Qwest offers cellular service through a partnership with Verizon. Qwest® One Number Service - a single phone number for a Verizon Wireless phone and Qwest landline phone. Calls will ring both the Qwest landline phone and the Verizon Wireless phone. Unanswered calls to a single voice mail box. In some cases it may be necessary to send a Subpoena or Court Order to both Qwest & Verizon.</p>
<p>Sprint / Nextel Communications Security & Subpoena Compliance 6480 Sprint Parkway MS: KSOPHM0216 Overland Park, KS 66251 (800) 877-7330 Main (Option 1) (816) 600-3111 Subpoena Compliance Group</p> <p>Immediate Response Requests (not Emergencies) (913) 315-8774 Fax (816) 600-3121</p> <p>Trials/Appealance CSTrialTeam@sprint.com</p> 	<p>CDMA</p>	<p>Virgin Mobile MVNO prepaid service – Sprint</p> <p>Send a Text Message: Virgin Mobile USA [10-digit phone number]@vmobl.com Example: 5551234567@vmobl.com</p> <p>Boost Mobile MVNO prepaid service – Nextel (iDEN) PTT service or CDMA service</p> <p>Send a Text Message: Boost Mobile [10-digit phone number]@myboostmobile.com Example: 2125551212@myboostmobile.com</p> <p>Kajeet & iWireless – MVNO prepaid service – Sprint</p> <p>Sprint offers an optional GPS location service: Family Locator http://www.nextel.com/en/services/gps/family_locator.shtml</p>    
<p>T-Mobile, USA Law Enforcement Relations 4 Sylvan Parsippany, NJ 07054 (973) 292-8911 Main (973) 292-8697 Fax ler2@t-mobile.com</p> 	<p>GSM</p>	<p>Send a Text Message: T-Mobile [10-digit phone number]@tmomail.net Example: 4251234567@tmomail.net</p>
<p>TracFone Wireless, Inc. Subpoena Compliance 9700 NW 112th Avenue Miami, FL 33178 (800) 820-8632 Main (305) 715-6932 Fax</p> 	<p>MVNO GSM or CDMA options</p>	<p>Also sold as Net10 & Safelink in some markets</p> <p>(800) 867-7183 Customer Care Center</p>  



LAW ENFORCEMENT TELEPHONE INVESTIGATIONS RESOURCE GUIDE

– Cellular, Satellite & VoIP Phone Providers







U.S. Cellular Subpoena Compliance Department One Pierce Place, Suite 800 Itasca, IL 60143 (630) 875-8270 Main (866) 669-0894 Fax (865) 777-8333 after Hours		CDMA	<p>Send a Text Message: US Cellular [10-digit phone number]@email.uscc.net Example: 4251234567@email.uscc.net</p> <p>Roaming partner with Verizon</p>
Cellco Partnership dba Verizon Wireless Custodian of Records 180 Washington Valley Rd. Bedminster, NJ 07921 (800) 451-5242 Main (888) 667-0028 Fax (Subpoenas) (908) 306-7501 Exigent Fax (908) 306-7491 Fax (Court Orders / Search Warrants)		CDMA	<p>INpulse is Verizon prepaid service Alltel – is also a Verizon company AirTouch – is also a Verizon company JitterBug – is also a Verizon company</p> <p>Send a Text Message: Verizon [10-digit phone number]@vtext.com Example: 5552223333@vtext.com</p> <p>Verizon offers an optional GPS location plan: Family Locator http://products.verizonwireless.com/index.aspx?id=fnd_familylocator</p> <p>  </p>
Globalstar Subpoena Compliance 461 S. Milpitas Blvd. Milpitas, CA 95035 (408) 933-4840 Main (408) 933-4844 Fax (877) 452-5782 Customer Care		Satellite	<p>Satellite Telephone Service Only</p> <p>Law Enforcement Technical Support: (408) 933-4144 Jose Jara (Office) (408) 828-0987 Jose Jara (Cell phone)</p>
Iridium Satellite ATTN: Orders LEA 8440 S. River Parkway Tempe, AZ 85284 USA (480) 752-1144 Main (480) 752-5130 Fax (866) 947-4348 Customer Care		Satellite	<p>Satellite Telephone Service Only</p> <p>Law Enforcement Technical Support: (602) 741-4224 Thomas Lopez (Cell phone) (877) 454-7631 Thomas Lopez (Pager)</p>
There are numerous VoIP providers – several currently popular VoIP providers are listed below:		VoIP	<p>Additional VoIP providers can be found here: http://www.myvoipprovider.com/Top_100_VoIP_Providers</p>



LAW ENFORCEMENT TELEPHONE INVESTIGATIONS RESOURCE GUIDE

– Cellular, Satellite & VoIP Phone Providers



Magic Jack http://www.magicjack.com/ YMax Communications ATTN: Lorraine Fancher 5700 Georgia Avenue West Palm Beach FL 33405 (561) 586-3380 Legal Compliance (888) 762-2120 Fax Lorraine.Fancher@vmaxcorp.com	 	VoIP	The Magic Jack resembles the appearance of a flash drive. You can simply plug it into a USB port of your computer and then plug in any kind of analog or cordless phone on the other end and you would be able to make unlimited local and long distance calls. Features include voice mail, call forwarding, conference calling, call waiting and caller ID.
Vonage http://www.vonage.com/ Hours of Operation: 24/7 Phone: 1-866-293-5674 Please state immediately that you are from a LEA with an emergency threat to life situation. Non-Emergency Email: SubpoenaProcessTeam@Vonage.com Phone: 732-231-6705 Fax: 732-202-5221 Vonage Holdings Corp. Attention: Legal Affairs Administrator - Legal Dept, 23 Main Street Holmdel, NJ 07733		VoIP	You can verify a phone number is a Vonage phone number by calling (732)377-3597. You must add a "1" before the number including the area code and the system will tell you if the number is a Vonage number or not. Emergency (life-threatening situation) Requests must be followed by the proper legal demand within 48 hours. We will verbally provide the information, and once we have received the proper legal demand, we will follow-up with a hard copy. Hours of Operation: 8:30 AM to 5:30 PM (Monday – Friday – ET) Response time for valid subpoena requests: 3-5 days Vonage requires special hardware in order to work - usually an Ethernet router with built-in telephone adapter. Once you sign up for a Vonage account, you can use a Web interface to view your call history and change your account settings.
Skype http://www.skype.com/ Skype Communications S.A.R.L 22/24 Boulevard Royal, L-2449 Luxembourg Tel: 01135226190920 lerm@skype.net		VoIP	The Skype application looks and works a lot like an instant messaging (IM) client. As with an IM client, users can change their on-line status, look at their contact list and decide who they want to talk to. In order to use these functions and to make calls, their computer has to be on and connected to the Internet, and their Skype application has to be running. Calls to other Skype users are free. Skype Mobile application can be used with Verizon smart phones with an active data plan. These calls use Verizon's 3G broadband connection.



LAW ENFORCEMENT TELEPHONE INVESTIGATIONS RESOURCE GUIDE

– Cellular, Satellite & VoIP Phone Providers



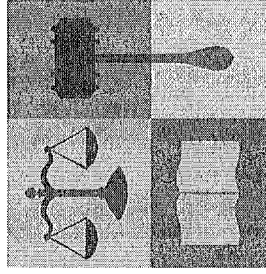
LEGAL FRAMEWORK:

United States Constitution 4th Amendment

Protects citizens against “unreasonable searches and seizures” by the Government.

Hierarchy of Protection

1. Transactional Records (name, number, billing records, etc.)
2. Numbers dialed from or to a phone.
3. Location information.
4. Content of stored communication (e-mail, voice mail, text messages, etc).
5. Content of telephone conversations (wiretap).



18 U.S.C. §§ 2701-2711 — STORED WIRE AND ELECTRONIC COMMUNICATIONS & TRANSACTIONAL RECORDS ACCESS

- **Section 2701:** It is a crime to intentionally access electronic communication without authorization.
- **Section 2702:** A provider of electronic communications may not disclose customer records to the government except as authorized by Section 2703, or if the provider reasonably believes an emergency involving immediate danger of death or serious bodily injury justifies disclosure. Penalties include fines, civil liability and imprisonment for 1 to 10 years.
- **Section 2703(b) (2).** A governmental entity may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.
- **Section 2703(c):** A court order, search warrant or customer consent is required for the release of records of electronic communications (including location information). A subpoena can be used to obtain transactional records, but not for location information.
- **Section 2703(d).** 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.

Refer to the complete United States Code sections for details: http://www.justice.gov/criminal/cybercrime/ECPA2701_2712.htm



LAW ENFORCEMENT TELEPHONE INVESTIGATIONS RESOURCE GUIDE

– Cellular, Satellite & VoIP Phone Providers



WEBSITE RESOURCES FOR PHONE RELATED INVESTIGATIONS:

Ask CALEA

Communications for Law Enforcement Act (CALEA). CALEA directs the telecommunications industry to design, develop, and deploy solutions that meet certain assistance capability requirements. As a law enforcement user you can create a free account and access CALEA's resources. Resources include provider contact information, cell tower location details, sample forms, etc.
<https://sw.askcalea.net/>



Find Cell Phone Providers for a particular region by Zip Code

Find and research all the cell phone companies licensed to serve your area. Enter your ZIP code to start your search.
<http://www.wirelessadvisor.com/>

Understanding Cell Phone Providers – Cnet

A comprehensive source of information with details about each of the major providers.
http://reviews.cnet.com/2719-3504_7-389-1.html?tag=page:page



<http://www.spooftcard.com/>

LE Contact: cmazur@teltechcorp.com (732) 838-1909

Locate Cell Towers

Find cell towers and the associated providers in a given area. Helpful when the location and time frame have been narrowed down, but the target's phone number is unknown. A Court Order for a "tower Dump" could provide valuable leads.
<http://www.cellreception.com/towers/>

Glossary of Cellular Phone Terms

A comprehensive list of terminology associated with cellular telephone related technology.
<http://www.wirelessadvisor.com/resources/glossary>

Phone Scoop

A resource with instructions to help navigate through various menus on a particular cell phone model to access address books, recent call history, features, options, accessories, etc.
<http://www.phonescoop.com/>

Internet Service Providers (ISP) Law Enforcement Contact Information

This confidential law enforcement site includes current contact information for ISPs and similar information services, specifically, contacts at the legal departments for law enforcement service of subpoena, court orders, and search warrants.
<http://www.search.org/programs/hightech/isp/> **How to trace an IP address:** <http://www.wikihow.com/Trace-an-IP-Address>

CONFIDENTIAL MATERIAL – LAW ENFORCEMENT SENSITIVE – DO NOT DISCLOSE

Revised 03-10-10 CF

Page 7



LAW ENFORCEMENT TELEPHONE INVESTIGATIONS RESOURCE GUIDE

– Cellular, Satellite & VoIP Phone Providers



Bank Card Services - 24 Hour Law Enforcement Contact Information

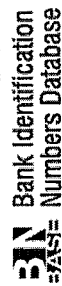
Phone equipment and services are usually paid for with credit or debit cards. The transactional records from these purchases can be very helpful in identifying purchasers and their associates, retail locations (a possible source of surveillance video) and other relevant purchases that may help develop leads in an investigation (e.g. Internet service providers, "Spoof" card purchases, gas stations used, etc.).



Visa	Accounts begin with "4"	1-800-FOR-VISA (367-8472)
American Express	Accounts begin with "37"	1-800-528-2121
Diner's Club	Accounts begin with "38"	1-800-525-9040
Discover	Accounts begin with "6"	1-800-347-3723
Master Card	Accounts begin with "5"	1-800-231-1750

Bank Identification Number Database:

<http://www.binbase.com/csv.php?module=search>



GLOSSARY OF TERMS:

CDMA - Code Division Multiple Access

CDMA and GSM are the names of competing cellular phone standards. CDMA phones are activated remotely, by the carrier, using the phone's serial number, known as the ESN. Since each carrier has a database of all the ESNs that are approved for its network, this lets most CDMA carriers refuse to activate phones not originally intended for their network. CDMA phone providers include Verizon, Sprint, US Cellular, MetroPCS and Cricket.

GSM - Global System for Mobile communications

GSM phones are associated with what's called a SIM card, or Subscriber Identity Module. This card, about the size of a fingertip and the thickness of a piece of paperboard, carries an encrypted version of all the information needed to identify the wireless account to the network. On most GSM phones the SIM card is usually under the battery. GSM phone providers include AT&T Mobility (including GoPhone) and T-Mobile. Unlike CDMA phones, GSM phones can be used internationally.

iDEN - Integrated Digital Enhanced Network (includes Push-to-Talk "PTT" walkie-talkie feature)

A wireless technology from Motorola combining the capabilities of a digital cellular telephone, two-way radio, alphanumeric pager and data/fax modem in a single network. Nextel is the brand name for Sprint's line of iDEN walkie-talkie enabled phones - this feature is called "Direct Connect". Boost Mobile is a subsidiary of Sprint Nextel, providing an economy prepaid service (MVNO) for the youth market, using the same iDEN technology as Nextel, and using Sprint Nextel's iDEN network. Boost also offers unlimited service using CDMA phones and Sprint Nextel's CDMA network.



LAW ENFORCEMENT TELEPHONE INVESTIGATIONS RESOURCE GUIDE

– Cellular, Satellite & VoIP Phone Providers



MVNO - Mobile Virtual Network Operator - Secondary seller

An MVNO is a cell phone carrier (such as a prepaid wireless carrier) that typically does not have its own network infrastructure and licensed radio spectrum. Instead, a smaller MVNO has a business relationship with a larger *mobile network operator* (MNO). An MVNO pays wholesale fees for minutes and then sells the minutes at retail prices under its own brand. An MVNO, therefore, is an MNO reseller. An MVNO is actually a customer of an MNO rather than a competitor. An MVNO can typically set its own pricing following agreed-upon rates with its contracted MNO. Boost Mobile, TracPhone, OnStar and JitterBug, for example, are all prepaid wireless MVNOs. AT&T Mobility and Verizon Wireless, for example, are MNOs. It is often beneficial to request records from the MNO verses the MVNO – especially with live tracking and cell tower records.

PCS – Personal Communications Service

Personal Communications Services (PCS) is a wireless phone service very similar to cellular phone service, but with an emphasis on *personal* service and extended mobility. The term "PCS" is often used in place of "digital cellular," but true PCS means that other services like paging, caller ID and e-mail are bundled into the service. While cellular was originally created for use in cars, PCS was designed from the ground up for greater user mobility. PCS has smaller cells and therefore requires a larger number of antennas to cover a geographic area. PCS phones use frequencies between 1.85 and 1.99 GHz (1850 MHz to 1990 MHz). Technically, cellular systems in the United States operate in the 824-MHz to 894-MHz frequency bands; PCS operates in the 1850-MHz to 1990-MHz bands.

SMS - Short Message Service – Text messages

SMS stands for **Short Message Service**. SMS is a method of communication that sends text between cell phones, or from a PC or handheld to a cell phone. The "short" part refers to the maximum size of the text messages: 160 characters (letters, numbers or symbols in the Latin alphabet). SMS is a store-and-forward service, meaning that when you send a text message to a target, the message does not go directly to your target's cell phone. The advantage of this method is that your target's cell phone doesn't have to be active or in range for you to send a message. The message is stored in the SMSC (for days if necessary) until your target turns their cell phone on or moves into range, at which point the message is delivered. The message will remain stored on your target's SIM card (GSM phones) until it is deleted.

SIM Card

GSM cellular phones require a small microchip, called a SIM card - Subscriber Identity Module, to function. Approximately the size of a small postage stamp, the SIM Card is usually placed underneath the battery in the rear of the unit, and (when properly activated) stores the phone's configuration data, and information about the phone itself, such as which calling plan the subscriber is using. When the subscriber removes the SIM Card, it can be re-inserted into another phone that is configured to accept the SIM card and used as normal. Each SIM Card is activated by use of a unique numerical identifier; once activated, the identifier is locked down and the card is permanently locked in to the activating network. For this reason, most retailers refuse to accept the return of activated SIM Cards. Common providers that require SIM cards include: AT&T Mobility, T-Mobile and Nextel.



LAW ENFORCEMENT TELEPHONE INVESTIGATIONS RESOURCE GUIDE

– Cellular, Satellite & VoIP Phone Providers



IMEI - International Mobile Equipment Identifier

A unique 15-digit number that serves as the serial number of the GSM handset. The IMEI appears on the label located on the back of the phone. The IMEI is automatically transmitted by the phone when the network asks for it. A network operator might request the IMEI to determine if a device is in disrepair, stolen or to gather statistics on fraud or faults.

ESN - Electronic Serial Number

The unique identification number embedded in a wireless phone by the manufacturer. Each time a call is placed, the ESN is automatically transmitted to the base station so the wireless carrier's mobile switching office can check the call's validity. The ESN cannot easily be altered in the field. The ESN differs from the mobile identification number, which is the wireless carrier's identifier for a phone in the network. MINs and ESNs can be electronically checked to help prevent fraud.

Cell Site

The location where the wireless antenna and network communications equipment is placed. A cell site consists of a transmitter/receiver, antenna tower, transmission radios and radio controllers. A cell site is operated by a Wireless Service Provider (WSP).

VoIP - Voice over Internet Protocol

VoIP (voice over IP) is an IP telephony term for a set of facilities used to manage the delivery of voice information over the Internet. VoIP involves sending voice information in digital form in discrete packets rather than by using the traditional circuit-committed protocols of the public switched telephone network. A major advantage of VoIP and Internet telephony is that it avoids the tolls charged by ordinary telephone service. Popular VoIP providers include Vonage, Skype and Magic Jack.

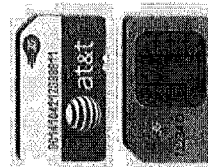
NOTE:

The information contained in this guide is law enforcement sensitive and should not be disseminated outside of the criminal justice system. Do not include with investigative reports.

Do not disclose this information in court anymore than is absolutely necessary to make your case.

Never disclose to the media these techniques – especially cell tower tracking. Simply state, "Through further investigation we were able to locate the suspect (or missing person)".

While every effort has been made to ensure the information contained in this guide is current and accurate, Fox Valley Technical College does not hold itself liable for any consequences, legal or otherwise, arising from the use of this Guide. Consult with your own agency and local prosecutor for legal advice before proceeding.



EXAMPLE OF A SIM CARD
FROM A
GSM PHONE



LAW ENFORCEMENT TELEPHONE INVESTIGATIONS RESOURCE GUIDE

- Cellular, Satellite & VoIP Phone Providers



SAMPLE CELL PHONE RECORDS PRESERVATION LETTER:

March 10, 2010

National Subpoena Compliance Center
AT&T Mobility
P.O. Box 24679
West Palm Beach, Florida 33416-467
(800) 635-6840 FAX (888) 938-4715

(OFFICIAL DEPARTMENT LETTERHEAD)

IMPORTANT:

Always call the provider after the
Preservation Letter has been sent
to them via fax to confirm that it
has been received and will be acted
on in a timely manner.

DO NOT DISCLOSE

RE: Court Order to Provide Telephone Records JCSO Case 10-1234

URGENT REQUEST FOR ASSISTANCE - CHILD ABDUCTION INVESTIGATION

The Jackson County Sheriff's Office is investigating a child abduction. We will be requesting telephone records which we believe will provide important evidence in our case. The court order, which will follow, will comply with all requirements outlined in United States Code, Title 18, Part I, Chapter 121, § 2703(d). The order will be obtained with a sworn affidavit which will include "specific and articulable facts".

We are sending this notice to request the records be pulled and held before they are lost and cannot be recovered. The court order will follow within 30 days.

Please call me immediately if these records are no longer available or if there are any problems.

SUBSCRIBER TELEPHONE NUMBER: (541) 555-1212 TIME PERIOD: 02-15-10 to current

We will be requesting:

- AT&T Mobility subscriber billing & account information – to include account notes.
- In-coming and out-going cell tower records.
- In-coming and out-going call detail records.
- Cell tower location information.
- All stored photographic or video images.
- All stored voice mail messages.
- In-coming and out-going text messages.

Respectfully,

Detective Joe Friday



LAW ENFORCEMENT TELEPHONE INVESTIGATIONS RESOURCE GUIDE

– Cellular, Satellite & VoIP Phone Providers



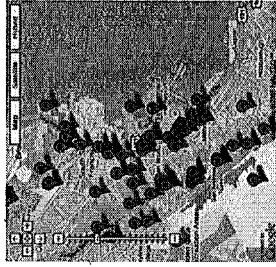
TOOLS FOR PLOTTING CELL TOWER LOCATION DATA:

Microsoft Streets & Trips – Free Trial Download (60 day)

<http://www.microsoft.com/streets/en-us/Trial.aspx>

Using Streets & Trips to Map Cell Towers:

1. Open Streets & Trips
2. Data Tab – select “Import Wizard”
3. Find the appropriate cell tower data file from the provider (Excel or .xls file)
4. Select the file
5. Click on Sheet 1
6. Review the dialog box and make sure the data is match to Latitude & Longitude
7. Click on Finish



Paraben Forensics Point 2 Point– Free Demo Download

(Demo has some limitations over the full version – plots on Google Earth)

http://www.paraben.com/catalog/product_info.php?cPath=25&products_id=404

GPS data points can show up in investigations from devices as well as subpoenaed cell phone records. Point 2 Point converts these data points to be read directly into Google Earth so investigators can quickly and easily visualize where these GPS locations are. Paraben's Point 2 Point is a point analysis tool that allows you to import GPS location data from call detail record spreadsheets, Device Seizure, or other GPS data points and export them to PDF or KML format for use with Google Earth. Imagine being able to take raw data from cell phone providers such as call detail records or GPS devices for review in a visual map for easy analysis.

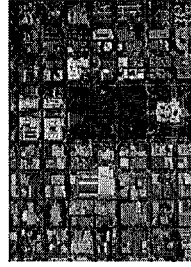
- Import and view data from Tower Location spreadsheets directly from the provider
- Import and view data in Google Earth Map Files (.kml)
- Export all imported data to either .kml files to be viewed with Google Earth or to .pdf files.

On-line Aerial Image Resources

Google Earth: <http://earth.google.com/>

Bing Maps: <http://www.bing.com/maps/>

(Select aerial view)



Fuller, Amber

From: Knight, Shawn
Sent: Wednesday, August 25, 2010 8:08 AM
To: shwnknight@yahoo.com
Subject: FW: Scanned image from AR-M257
Attachments: AR-M257_20100825_043704.pdf

From: sharpscan@oaklandnet.com [<mailto:sharpscan@oaklandnet.com>]
Sent: Wed 8/25/2010 5:37 AM
To: Goodfellow, Ryan M.; Knight, Shawn
Subject: Scanned image from AR-M257

DEVICE NAME:
DEVICE MODEL: SHARP AR-M257
LOCATION:

FILE FORMAT: PDF G4
RESOLUTION: 200dpi

Attached file is scanned image in PDF format.
This file can be read by Adobe Acrobat Reader.
The reader can be downloaded from the following URL:

<http://www.adobe.com/>



Last updated February 15, 2006

MySpace.com

Official Law Enforcement Officers Investigators Guide

Mailing Address: Custodian of Records MySpace.com 1333 2nd Street, First Floor Santa Monica, CA 90401	LEO Telephone: Phone: 310.917.4945 Fax: 310.394.4180
LEO E-mail Address: lawenforcement@myspace.com	

Table of Contents

Preface.....	3
A. Introduction.....	4
B. About MySpace.com.....	5
C. What Information MySpace.com Collects and Retains	6
D. Current MySpace.com Retention Periods.....	7
i. Active Accounts.....	7
ii. Deleted Accounts.....	7
E. Requests to Preserve Records.....	8
F. How to Request Records/Information	9
G. What Information You Will Receive and How to Interpret It.....	10
H. Sample Forms	12
i. Sample Subpoena.....	12
ii. Sample Preservation Request Letter.....	13
iii. Sample Consent Form	14
I. Understanding IP Addresses.....	15
J. Websites and Resources	16

Preface

This Law Enforcement Officers Guide is for law enforcement investigators interested in obtaining data collected and retained by the website MySpace.com ("MySpace"). The Guide is designed to provide information and assistance to law enforcement officers about what information is collected, how it is collected and how long it is retained by MySpace. It is also designed to assist law enforcement investigators to understand how to request properly the information they are subpoenaing. This guide has been prepared with the assistance of Parry Aftab of WiredSafety.org.

A. Introduction

The police have a significant role to play in achieving security of information and electronic commerce objectives through strong and effective partnerships, as well as proactive and innovative efforts. MySpace supports the vision of providing a safer and more secure environment for all users of the MySpace website. In support of and in the spirit of this vision, this Guide assists MySpace's partners in the law enforcement community.

MySpace is committed to a high level of cooperation with law enforcement to assist in investigating and identifying those involved in electronic crime and other crime with an electronic component. MySpace is also dedicated to assisting in the education of police staff and the public to enhance user safety. Therefore, MySpace created this Guide, which is designed to explain what information is retained and can be provided in response to a subpoena, and how the process works.

MySpace reserves the right to change any of the policies stated in this Guide at any time without notice. This Guide is intended solely for use by bona fide law enforcement agencies and may not be distributed to any other person or organization without the express written authorization of MySpace. MySpace will require verification that the person requesting this Guide is a bona fide law enforcement officer or acting on behalf of a law enforcement agency or prosecutor's office. This Guide is the property of MySpace and is protected by copyright laws. The contents of this Guide are confidential.

B. About MySpace

MySpace is a free website designed primarily for social-networking. It allows users to set up their own profile pages, which can include lists of their favorite musicians, books and movies, photos of themselves and others and links to pages within and outside the MySpace environment. There are many third party features which can be used with a MySpace profile, but which are not controlled by MySpace. MySpace has a privacy policy and terms of use agreement which control posts and activities on our website, such as forbidding nudity, violence, or offensive subject matter. It also has a team of employees assigned to enforce those policies and handle user inquiries.

MySpace does not charge its users to set up their profiles or establish an account. It does not require or accept credit card or other payments, and does not independently verify the identity of its users. It is possible for a user to establish a false identity or name. Because of this anonymity, even with a valid subpoena from law enforcement, the information may not be able to be provided by MySpace. Nonetheless, MySpace is committed to assisting with the investigation to the full extent consistent with applicable law and its website's privacy policies.

C. What Information MySpace Collects and Retains

Most profile information is publicly viewable and available. Publicly available information includes journal entries (in most cases unless the profile owner has elected to make the entry "private"), images, user comments, friend lists and public profile information such as first name, headline, music, movies, books and all other public sections on a MySpace profile.

In order to make an electronic copy of the public components of the profile in question, the investigator should save the web page(s) and files on her computer. While viewing the profile in question, click your browser's "File" menu tab (in the upper left-hand corner) then drop down to and click "Save As". Make sure to do the same for all journal entries and the image gallery.

Subpoenaing Private Information

To request private (non-public) information from MySpace about a specific profile or user, we require a subpoena, search warrant or other legal process. The following list is private content that is not publicly accessible. Some of the content is provided by the users themselves upon registration when updating profiles. Other items are collected by the site automatically or involve communications on MySpace.

These include:

- IP logs (recorded at time of login)
- Date profile created
- Dates and times of login (PST)
- E-mail address provided by user
- Zip code provided by user
- Name provided by user
- Private Messages
- Private blogs

Please note that the information provided by the user may not necessarily be accurate. Users do not need to confirm their email address, nor is this information verified by MySpace. Computer savvy users may also fake IP addresses if they use a proxy server.

D. Current MySpace Retention Periods*

MySpace retains information on its users for certain periods of time. To the extent law enforcement seeks information relating to publicly available or private information on MySpace, the retention periods should be noted so that MySpace can respond to the subpoena in the most helpful manner. To the extent information that was scheduled to be deleted needs to be retained by MySpace due to an on-going law enforcement investigation, MySpace will do so in response to a written law enforcement preservation request. (see Section E below)

i. Active Accounts

Data and Images on an active account

Data and images on an account are maintained as long as the user has not removed or edited the content from the profile. MySpace does not retain information that is altered on or removed from an active profile. Once a change is made, existing information is overwritten.

IP Logs

Each IP Log is available for up to ninety days after the applicable login on the account.

Private Messages in an Active Account User's Inbox

Private messages are retained until the user removes them. MySpace cannot recover the removed message, but could attempt to retrieve it elsewhere only if it is in another user's Sent Mail and MySpace knows the identity of the sender.

Sent Mail

Sent mail is retained for 14 days.

Trash Mail

Trash mail (mail that has been read and discarded) is retained 30 days or less. Note that users can empty their trash at any time after which the data is permanently lost.

ii. Deleted Accounts

No mail (inbox or sent mail) is available for deleted accounts.

User ID, IP Address, Login date stamps are retained for up to 90 days after account deletion.

Profile information is available for up to ten days after account deletion.

* Please note that all retention periods are estimated and may vary depending on system conditions and other circumstances.

E. Requests to Preserve Records

While MySpace's normal retention periods for various account information appears above, in special circumstances, it can retain records for longer periods of time to enable law enforcement to obtain the requisite subpoenas, court orders or to continue with an active investigation. In order for MySpace to preserve records, the law enforcement agency must submit a signed letter on law enforcement letterhead requesting that MySpace preserve the records. Please use the MySpace law enforcement telephone number and e-mail contact information that appear on the cover of this Guide to inquire about this procedure.

Attached in our form section is a sample letter for a preservation request that can be faxed to MySpace. Once an account has been preserved, the following will occur unless other arrangements are made with MySpace and indicated in the letter:

- The account will still be publicly viewable
 - The user will not be able to log into her account
 - Information in the Sent Mail/Trash folder is still subject to automatic deletion.
- MySpace can only preserve a currently active (non-deleted) account.

If restricting the user's access to the profile will impede an investigation, you may request that private messages be output to a flat file for preservation before a subpoena is served. You must specifically request in the letter that the user **not** be notified of the investigation if you do not want the subject account to be locked.

F. How to Request Records/Information via Court Order/Subpoena

MySpace will accept subpoenas delivered by fax or mail. MySpace will respond to out-of-state U.S.-based subpoenas and court orders. Requests from non-US law enforcement agencies may be handled differently; please contact the MySpace law enforcement office before serving the subpoena request. The fax and e-mail addresses are located on the cover of this Guide, and are listed below.

When law enforcement officials draft a subpoena in order to request private information, it should be as specific as possible. MySpace has more than 50 million users and therefore the 'FriendID' of the relevant account should be in the subpoena. The FriendID can be located in the web address of the profile in question.

Example of FriendID for Tom's profile:

<http://www.myspace.com/index.cfm?fuseaction=user.viewProfile&friendID=6221&Mytoken=20050518161358>

The above FriendID in this example is '6221'. This unique number allows us to locate the profile. If the profile appears as 'MySpace.com/Tom', click on the 'View More Pics' link. This will display the following link:

<http://viewmorepics.myspace.com/index.cfm?fuseaction=user.viewPicture&friendID=6221&friendName=Tom&Mytoken=20050829192700>

The FriendID can then be located in the URL.

Please be as specific as possible in the subpoena as to what information is being requested. For example, "Request for FriendID 6221 IP logs, email address and private messages located in the user's Inbox and Sent Mail Records for date range 5/14/2006-6/16/2006."

The preferred way for MySpace to respond to the subpoena is via E-mail because the data is presented in an Excel spreadsheet. Therefore, if possible, specify on the subpoena the email address to which results can be sent and where an authentication letter can be faxed.

The MySpace user will still have access to his/her account after MySpace has been served with legal process, unless MySpace has been requested to lock and preserve the account. If locking the account will impede the investigation, please contact MySpace in advance to see if special arrangements can be made. Please note that if MySpace does not lock the account, the user has the ability to delete, modify and edit the account data.

Our fax number for subpoenas, warrants and other legal processes is 310.394.4180; the email address is lawenforcement@myspace.com.

G. What Information Can Be Provided in Response to a Subpoena and How to Interpret It

Deciphering the information sent from MySpace

Email Address

Please note that an email address consists of two parts: A username and then the domain that hosts the email account.

Example: Abuse@MySpace.com

'Abuse' is the username and all information after the '@' belongs to the domain (which in this case is MySpace.com). Therefore, you should contact MySpace.com to make inquiries about the username 'Abuse'.

IP Logs

IP Logs also include a date stamp. All IP logs provided by MySpace.com are Pacific Standard Time zone.

Example: 67.134.143.254 08/22/2005 3:15 PM PST

You can find out which Internet Service Provider the IP address belongs to by going to a Reverse DNS site, such as <http://www.whois.sc> and entering the IP address into a search field.

The IP Address in the example above (67.134.143.254) generated the following result:
Qwest Communications QWEST-BLKS-5 (NET-67-128-0-0-1)
67.128.0.0 - 67.135.255.255

That means the IP address belongs to Qwest Communications. Qwest Communications could be contacted to provide the information about what individual or company was using that IP address at that date and time.

MySpace has included more resources later in this document about looking up IP addresses. Please refer to the section titled 'Understanding IP Addresses'.

Private Messages

There will be two separate tabs on the bottom of the Excel spreadsheet for the Private Messages. One is the 'Sent From User' and the other is 'To User'. These are messages that are sent from the user in question to other users and that are located in the user's "Sent Mail" records, and messages from other users to the user in question that are located in the user's "Inbox" records, respectively.

The spreadsheet for private messages will have the following five headers:

ToUserid	FromUserid	Subject	Body	CreatedDate
----------	------------	---------	------	-------------

ToUserid is the FriendID of the account the message is sent to.

FromUserid is the FriendID of the account the message is sent from.

Subject is the subject line of the message in question.

Body is the actual content of the message.

CreatedDate is the date stamp of the message.

Example:

ToUserid	FromUserid	Subject
6221	222345245322	RE: Welcome to MySpace.com

Body

Thank you Tom for the welcome!

----- Original Message -----

From: <A

HREF='http://www.myspace.com/index.cfm?fuseaction=user.viewProfile&friend
ID=6221&Mytoken=20050423222742'>Tom Date: Apr 23, 2005 4:49 PM
Hi, My name is Tom! Welcome to MySpace

CreatedDate

4/23/2005 22:29

Please note the '----- Original Message -----' in the body of the message and the 'Re' ("Regarding") in the subject line shows that the user in question is responding to an existing private message sent to him. The responding email shows who the original sender is, as well as the time and date sent.

H. Sample Forms

i. Sample Subpoena

Example of a Subpoena Duces Tecum:

IN THE SUPERIOR COURT OF THE STATE OF ARIZONA
IN AND FOR THE COUNTY OF WIDGETVILLE

In the Matter of the Appearance
and Attendance Before the Grand Jury

Subpoena Number
Subpoena Duces Tecum

The State of Arizona, to:

MySpace.com
ATTN: Custodian of Records
1333 2nd St, First Floor
Santa Monica, CA 90401
Phone: 310 917 4945
Fax: 310 394 4180

You are hereby commanded pursuant to appear before the inquest of the Grand Jury which will be in session in the above-entitled court, by coming to (Address of the Court house) on the [] day of , 200[], at the hour of [], to testify and give evidence in all such matters and things as may be there inquired of you; and to act on hearings of said Grand Jury until by them excused, and to bring with you:

- 1) IP Logs (recorded at time of login) for Friend ID #####
- 2) Dates and times of login (PST) for Friend ID #####
- 3) Subscriber information for Friend ID #####
- 4) Private messages in the user's inbox, trash and sent mail for Friend ID #####

Compliance may be made either on the specified date by delivery to the Grand Jury or prior to that date by delivery to (Your Name), (Address), (Phone and Fax), (EMAIL ADDRESS), hereby made an agent of the Grand Jury in the pending investigation to which the subpoenaed items relate, for the purpose of receiving, examining and maintaining said items.

You are cautioned that disclosure of any matter attending a Grand Jury proceeding, including disclosure of your receipt of or compliance with this subpoena, is a crime.

Of this, fail not, under penalty for contempt of the court.

Witness my Hand and Seal of said Court this [] day of [], 200[].

Clerk of the Superior Court

ii. Sample Preservation Request Letter

(Must be on law enforcement department letterhead)

Custodian of Records
MySpace.com
1333 2nd Street, First Floor
Santa Monica, CA 90401

Re: Preservation Request

Dear Custodian of Records:

The below listed account/profile is the subject of an ongoing criminal investigation at this agency, and it is requested that said account/profile and all related records, communications and data, and any other information contained therein, be preserved pending the issuance of a search warrant or other legal process. (Specify any information you may want here, see suggested wording for subpoena and warrant requests above.) I understand that MySpace.com will lock the profile/account in question, thereby rendering the account inaccessible to its owner.

Profile URL:
FriendID:

If you have any questions concerning this request please contact me at [insert e-mail address and phone contact]

Thank you for your assistance in this matter.

Sincerely,
(Your Signature)
(Your Name Typed)
(Your Title Typed)

In some cases, a MySpace user may consent to a law enforcement request for information. This can facilitate the process, and avoid the investigation team's need to obtain a warrant, court order or subpoena

iii. Sample Consent Form

(Must be on the investigating agency or department letterhead)

I, "XYZ", being duly sworn, on this [insert date] do hereby state the following:

I have one or more profiles on MySpace.com.
The URLs / FriendIDs are:

I understand that the "ABC" agency is conducting an official criminal investigation and has requested that I grant my consent to authorize the "ABC" agency to access, request, receive, review, copy and otherwise utilize, as they deem appropriate, all information of any kind held by MySpace.com relating to my MySpace.com profiles/accounts.

I hereby authorize MySpace.com to provide to any agent of the above referenced agency, any and all records relating to my MySpace.com profile/account, whether now existing or hereafter created, including, without limitation: (Please list each type of information you are requesting. See suggested requests above.)

Pursuant to this Consent, I waive any claims against, indemnify and hold harmless MySpace.com, its affiliates, and their respective directors, officers, agents, and employees from and against any claims, damages or expenses relating to or arising from, in whole or in part, the disclosure of such information, records and data.

I have not been promised anything in exchange for providing this consent and authorization.

In witness whereof, the undersigned makes the above statements under penalty of perjury.

Member Signature and Printed Name

Date

Law Enforcement Witness Signature, Printed Name
and Printed Title

Date

I. Understanding IP Addresses

Most IP addresses are temporarily provided by the user's Internet service provider. You can search for the owner of any range of IP addresses by doing a "Whois" lookup. Here are some suggested websites to search IPs.

<http://www.whois.sc>

<http://www.networksolutions.com/cgi-bin/whois/whois>

<http://www.arin.net/whois/arinwhois.html>

<http://www.ripe.net/db/whois.html> (Europe)

<http://www.apnic.net/apnic-bin/whois.pl> (Asia Pacific)

<http://www.nsiregistry.com/>

<http://www.registrars.com/static/whois/index.shtml>

<http://www.nic.mil/dodnic/>

Each ISP has an investigator's guide of its own, advising law enforcement agencies how to request information from them about one of their subscribers or users of their services. You may want to contact the ISPs in advance of any investigation so you have the information on hand when needed.

J. Websites and Resources

www.myspace.com/misc/safetytips.html - MySpace.com's Safety Tips section which includes a section dedicated to parents concerned about their child's Internet use.

United States Department of Justice, Office of Justice Programs, National Institute of Justice, publishes an investigative guide for electronic crime. The information contained in Electronic Crime Scene Investigation-A Guide for First Responders (available free of charge and downloadable from the Department of Justice website (www.ncjrs.org/pdffiles1/nij/187736.pdf)) helps line officers perform their jobs.

www.wiredsafety.org - Resource for online safety, education and law enforcement assistance.

www.cyberlawenforcement.org - WiredSafety's law enforcement website.

Fuller, Amber

From: hollycyuen@yahoo.com
Sent: Wednesday, August 25, 2010 1:13 PM
To: Knight, Shawn
Subject: Fw: American Express Charges for 8/25/10
Attachments: American Express.doc

Thank you!

Sent via BlackBerry by AT&T

-----Original Message-----

From: Christina Yuen <kristinajyuen@yahoo.com>
Date: Wed, 25 Aug 2010 12:25:20
To: Holly Yuen<hollycyuen@yahoo.com>
Subject: American Express Charges for 8/25/10

American Express – 1028

Time Vendor Amount Zip Code Address

8:57 PM Conoco Phillips/76 \$76 94605 3101 98th Ave, Oakland, CA 94605. (510)
635-2374

8:39 PM Quikstop Market #51 - Pump \$100 Oakland, CA

8:53 PM Valero \$75 California

9:06 PM Valero \$75 California

Charges will post 48 hrs after transaction

American Express – 1028

8/25/2010

Time	Vendor	Amount	Zip Code	Address
8:57 PM	Conoco Philips/76	\$76	94605	3101 98th Ave, Oakland, CA 94605. (510) 635-2374
8:39 PM	Quikstop Market #51 - Pump	\$100		Oakland, CA
8:53 PM	Valero	\$75		California
9:06 PM	Valero	\$75		California

Charges will post 48 hrs after transaction