California Association of Hostage Negotiators Presentation

June 5th, 2014

Aaron Edens

Police Technical

661 Poplar Street

Terre Haute, IN 47807

(812) 232-4200

[aedens@policetechnical.com](mailto:aedens@policetechnical.com)

[www.policetechnical.com](http://www.policetechnical.com)

**Contents**

[About the Instructor: 1](#_Toc390067501)

[Thank You: 1](#_Toc390067502)

[Introduction 2](#_Toc390067503)

[Controlling the Digital Perimeter 5](#_Toc390067504)

[The Elements of a Communications Shut Down Order 6](#_Toc390067505)

[Potential Consequences of Using the Communications Shut Down Order 9](#_Toc390067506)

[Limitations of a Communications Shut Down Order 9](#_Toc390067507)

[Provider Capabilities for Barricaded Suspect Situations 10](#_Toc390067508)

[Specific Provider Capabilities 12](#_Toc390067509)

[AT&T 12](#_Toc390067510)

[Cricket 13](#_Toc390067511)

[Metro PCS 14](#_Toc390067512)

[Sprint 15](#_Toc390067513)

[T-Mobile 16](#_Toc390067514)

[Verizon 17](#_Toc390067515)

# About the Instructor:

Aaron Edens is a retired Police Officer from the City of Hayward, California. He spent six years as an Intelligence Unit Detective assigned to the FBI-Joint Terrorism Task Force.  During that time he investigated international terrorism and Southwest Asian organized crime and major narcotics trafficking.  Additionally, Mr. Edens spent 10 years on the department’s Special Response Unit as a Tactical Medic and Team Leader.

Mr. Edens has been a certified mobile phone examiner since 2005 and has completed over 1000 forensic examinations.  Officer Edens is the Lead Cell Phone Investigations Instructor for Police Technical, a national law enforcement training company. He has taught mobile phone investigative techniques to thousands of law enforcement officers, analysts, and prosecuting attorneys.

## Thank You:

Mr. Edens would like to thank Hamilton County (TN) Sheriff’s Department Detective Ed Merritt. Detective Merritt researched the capabilities of the major cellular service providers and then shared the information for the benefit of the entire law enforcement community.

# Introduction

Current communication tactics and methodologies for negotiators are losing their relevancy and applicability. In many tactical situations involving negotiators there are no landline phones into a target residence. According to the Cellular Telephone Industry Association of America, 38.2% of households in the United States are wireless only. Despite this fact, the negotiations element of many law enforcement agencies are still focused on initiating communications using a landline phone.

Alternately, many law enforcement agencies rely heavily on the use of the throw or rescue phone. However, the use of these devices come with their own set of problems:

* The device has to be delivered into the residence. This may expose tactical operators to increased risk.
* The use of robots to deliver the device can be problematic based on the features of the building, wireless reception and interference, and battery issues. Additionally, the introduction of a robot can have consequences in situations involving suspects with mental illness such as paranoid schizophrenia.
* The device is inherently viewed as untrustworthy by the suspect. It is ‘ours, not ‘theirs.’
* The technology is big and bulky. People are used to small technology and not something that comes in a small Pelican® case attached to 100 yards of armored cable.

Cell phones and social media have changed the rules of crisis negotiation. These technologies have also brought with them a number of challenges. For example, on September 8th, 2012 in Denver, Colorado two suspects entered a store to commit a robbery. Law enforcement was alerted of the in-progress crime and the suspects fired shots at the responding officers. Investigators subsequently learned one of the suspects had an older brother who had been killed by police during a similar hostage taking incident. One suspect communicated to a family member ‘I’m not coming out, just tell my family I love them. If I do come out I’m going to be shooting.’

While inside the business, the suspects were able to summon family and friends to the scene using social media. The suspects communicated with their associates, bypassing the law enforcement negotiators. They also were able to update their Facebook® account and post a ‘selfie’ from inside the store.



SOURCE: http://denver.cbslocal.com/2012/09/08/standoff-suspect-posted-on-facebook-throughout-ordeal/

Failing to control the mobile device and social media contacts outside of negotiations channels compromises the perimeter. Most law enforcement tactical teams are familiar with controlling the physical perimeter but fail to control the digital perimeter. The results of failing to control the suspect’s communications could be disastrous.

In addition to summoning family and friends to the scene, suspects may be able to contact attorneys, media, and supporters. Perhaps most troubling is the potential for suspects to communicate the location and actions of tactical team members deployed to the scene.

On June 22, 2011 in Ogden, Utah a barricaded suspect with a hostage used Facebook to communicate with family and friends. During the 16 hour standoff, the suspect make six posts to his Facebook account, received at least 100 comments, and added six new friends to his account. One of the posts on the social network advised him where a SWAT officer was concealed. "Thank you homie. Good looking out."



SOURCE: http://abcnews.go.com/Technology/utah-gunman-updates-facebook-status-standoff-salt-lake/story?id=13903161

# Controlling the Digital Perimeter

There are methods for leveraging existing communications technologies for an advantage during pre-planned operations and emergent tactical situations. One evolving method is the use of a communications shut down order for pre-planned operations such as high risk warrant service.

The method of most deployments of SWAT personnel for pre-planned operations presents an inherent operational security risk. Many law enforcement agencies stage their tactical, command, and support elements a short distance away from the target location. This allows for final equipment and communications checks and loading the team into or onto the exterior of armored response vehicle in a relatively ‘secure’ area. Deploying tactical operators from the exterior of a vehicle permits rapid deployment and lessens the chance of an injury or delayed deployment as multiple officers try to exit the interior of a vehicle. However, this method also exposes officers to observation by those in the area who may be sympathetic to the suspect and alert him of the impending arrival of the tactical team. Make no mistake about it, the sight of 20 armed and armored tactical operators hanging off the sides of a Bear® armored vehicle immediately draws the attention of those in the area. The intentions, and likely the destination, of the vehicle and team are likely to be immediately apparent to the criminally minded who observe them. This may cause some to attempt to alert the target suspect resulting in the suspect arming himself, barricading himself, fortifying existing barricaded positions, and destroy the very evidence a warrant authorizes a search for.

In order to mitigate the risk to law enforcement officers serving warrants considered high-risk, many jurisdictions are permitted via judicial authorization to waive certain statutory requirements. The most commonly sought waivers are the ‘knock notice’ or ‘knock and announce’ requirement and any statutory time limitations for warrant service, commonly called ‘night service authorization.’ The same factors used to justify the waiver of ‘knock notice’ and ‘night service authorization’ can be used to justify restricting the suspect’s mobile phone service prior to the warrant service in order to prevent them from being alerted to the impending arrival of the tactical team.

A communications shut down order can be built into a search warrant affidavit or may be sought separately depending on local or state requirements. The shutdown order directs a cellular service provider to disconnect service to the suspect’s mobile device to prevent them from being alerted.

With proper pre-planning, the implementation of a communications shut down order has two primary benefits. The first benefit is preventing the suspect from being alerted to the presence of a tactical team. The second benefit is it limits the ability of the suspect to communicate with anyone outside of the incident. Many law enforcement officers are unaware that a mobile phone with no service is still able to call 911. This is an ideal situation for negotiators as the suspect’s communications are isolated to outgoing calls to a Public Safety Answering Point that can then be routed to the negotiations elements.

## The Elements of a Communications Shut Down Order

As noted, a shutdown order is based on the same factors that would be used to justify ‘night service’ or ‘no knock’ authorization. For example:

*Based on the violent nature of the crime under investigation, Smith’s prior arrests for weapons and violent crimes against persons, Smith’s self-admission to being a member of a criminal street gang, the observation of Smith being armed with a handgun, and his statements regarding his intent to violently resist apprehension to two separate informants, I have come to the belief the execution of a search warrant, should it be granted, will pose a high risk of injury or death for the law enforcement officers executing it.*

Additional justification may be based on prior knowledge of the suspect and the target area:

*The tactics of the HPD SRU are to deploy the tactical elements of the team from a ballistic resistant armored rescue vehicle. The team members routinely ride on the outside of the vehicle in order to rapidly and simultaneously deploy to the target location. The presence of an armored rescue vehicle with tactical operators on the outside of the vehicle is an attention grabbing site. This attention frequently causes those in proximity to either yell, text message, or make cellular telephone calls to associates, friends, family members, or members of criminal groups to warn them of the presence and impending deployment of the tactical team. Your affiant believes this may occur even during late night or early morning warrant service as Smith’s residence is notorious for vehicle and foot traffic in and around it at all hours of the day and night.*

The shutdown order has an anticipatory clause that disconnects service at the direction of the affiant or their designee. The incorporation of a designee is important as the person who actually contacts the provider may not be the same person who was the affiant on the search warrant.

*Your affiant is aware, through prior training and experience, cellular service providers have the ability to forcibly disconnect a mobile phone from their network. To minimize the risk of Smith being warned of the impending arrival of the tactical team and arming himself, barricading himself inside the residence, fortifying an existing barricade, and/or destroying evidence, your affiant requests judicial authorization to compel Smith’s cellular service provider, Verizon Wireless, to disconnect service to his mobile phone at the direction of the affiant or a designee.”*

It may be important to address concerns the reviewing magistrate or judge may have with forcibly disconnecting the suspect’s mobile phone service. Proactively addressing these concerns may mitigate any judicial concern.

*Your affiant knows from prior training and experience that even after a phone has had service disconnected it is still able to make emergency calls to 911. In the event Smith barricades himself inside his residence he would be unable to make any calls other than those to the 911 public safety answering point which would then be routed to the HPD SRU Crisis Negotiation Team.*

The communications shutdown may not be effective if the initiating law enforcement agency waits until the final approach of the tactical team. The cellular service provider should be served with the order well in advance of the execution of the tactical entry. The cellular service provider should be contacted after the service of the order to confirm receipt, explain the intentions and expectations, and determine a realistic time frame for them to comply with the order.

## Potential Consequences of Using the Communications Shut Down Order

There is a possibility the suspect may be alerted if they are using the phone at the time the cellular service provider terminates service. However, the risk is minimal and it is unlikely they would take any offensive or defensive actions as a result of their phone being shut off.

Similar to disconnecting other utilities such as electricity and water, disrupting communications may agitate a situation.

## Limitations of a Communications Shut Down Order

Temporarily suspending service from the cellular service provider does not necessarily limit the suspect from using other communications modalities. Specifically, the suspect may still be able to communicate using Wi-Fi internet connections from a residential or commercial internet provider. Disrupting cellular service:

* Does NOT impair Wi-Fi communications through third party applications such as Skype, What’sApp, or SnapChat.
* Does NOT impair Wi-Fi communications through social media

An additional consequence of the communications shutdown order is the loss of other communications tactics and techniques discussed in the following section.

# Provider Capabilities for Barricaded Suspect Situations

Cellular service providers have the ability to leverage their existing infrastructure and assist law enforcement with a number of different technologies to assist negotiators. Even though many of the cellular service providers employ nearly identical equipment their capabilities vary. The main service provider capabilities of interest to law enforcement negotiators include:

* Temporarily Block All Incoming Calls-The ability to temporarily block all incoming calls to the target phone number. This does not impact the ability to make or receive phone calls or text messages from other Wi-Fi services such as Skype or texting applications. For many providers, shutting down incoming phone calls means calls from all phones, including those used by the negotiator.
* Temporarily Block All Outgoing Calls-Some providers are able to restrict outgoing calls so the suspect cannot place a phone call to any phone number. Other providers can configure outgoing phone calls so no matter what phone number is dialed from the target the call is routed to the negotiator. This is referred to as a "ring down."
* Temporarily Suspend Text/Data-Temporarily suspend SMS text messages, MMS multimedia messages, and data connectivity. Most providers have the ability to restrict incoming and outgoing text messages, multimedia messages, and to shut down internet connectivity. This feature only works on the services of the cellular service provider. It does not impact third party Internet services. In order to prevent a suspect form communicating using these methods it may be necessary to identify and disconnect the Internet service used by the device and/or those in the area around the incident.
* Disable Call Waiting-Most, but not all, of the major cellular service providers can temporarily disable call waiting. This prevents negotiations from being interrupted by incoming phone calls from concerned family or friends.
* Shut It All Down-Temporarily suspend all account activity. If this tactic is used, the public safety answering point (PSAP) that accepts 911 calls should be alerted. This can be problematic for large jurisdictions or in areas where 911 calls are taken by another agency than the agency with jurisdiction over the incident (e.g. consolidated PSAPs, Highway Patrol/State Police 911 call centers.) Similar to the other modifications to the targeted mobile device, temporarily suspending all cellular service activity will not affect the Wi-Fi capabilities of the mobile device. It can still be used to communicate via VOIP applications or text message services independent of the service provider's restrictions.

# Specific Provider Capabilities

## AT&T

|  |  |
| --- | --- |
| Temporarilyblock all inbound calls to handset | Y |
| Can you allow calls from Negotiator only | N |
| Can all inbound calls be routed to another number | N |
| Temporarily suspend all outbound calls | Y |
| Can all attempted outbound calls be routed to Negotiator | Y |
| Temporarily suspend SMS, MMS, Data | Y |
| Turn off call waiting | N |
| Temporarily suspend ALL account activity | Y |

## Cricket

|  |  |
| --- | --- |
| Temporarilyblock all inbound calls to handset | Y |
| Can you allow calls from Negotiator only | N |
| Can all inbound calls be routed to another number | ? |
| Temporarily suspend all outbound calls | Y |
| Can all attempted outbound calls be routed to Negotiator | Y |
| Temporarily suspend SMS, MMS, Data | Y |
| Turn off call waiting | Maybe |
| Temporarily suspend ALL account activity | Y |

## Metro PCS

|  |  |
| --- | --- |
| Temporarilyblock all inbound calls to handset | Y |
| Can you allow calls from Negotiator only | N |
| Can all inbound calls be routed to another number | N |
| Temporarily suspend all outbound calls | Y |
| Can all attempted outbound calls be routed to Negotiator | N |
| Temporarily suspend SMS, MMS, Data | Y |
| Turn off call waiting | Y |
| Temporarily suspend ALL account activity | Y |

## Sprint

|  |  |
| --- | --- |
| Temporarilyblock all inbound calls to handset | N |
| Can you allow calls from Negotiator only | N |
| Can all inbound calls be routed to another number | N |
| Temporarily suspend all outbound calls | Y |
| Can all attempted outbound calls be routed to Negotiator | Y |
| Temporarily suspend SMS, MMS, Data | Y |
| Turn off call waiting | N |
| Temporarily suspend ALL account activity | Y |

## T-Mobile

|  |  |
| --- | --- |
| Temporarilyblock all inbound calls to handset | Y |
| Can you allow calls from Negotiator only | N |
| Can all inbound calls be routed to another number | N |
| Temporarily suspend all outbound calls | Y |
| Can all attempted outbound calls be routed to Negotiator | Y |
| Temporarily suspend SMS, MMS, Data | Y |
| Turn off call waiting | Y |
| Temporarily suspend ALL account activity | Y |

## Verizon

|  |  |
| --- | --- |
| Temporarilyblock all inbound calls to handset | Y |
| Can you allow calls from Negotiator only | N |
| Can all inbound calls be routed to another number | ? |
| Temporarily suspend all outbound calls | Y |
| Can all attempted outbound calls be routed to Negotiator | Y |
| Temporarily suspend SMS, MMS, Data | Y |
| Turn off call waiting | Y |
| Temporarily suspend ALL account activity | Y |