



1401 Eye Street, NW
Seventh Floor
Washington, DC 20005

Telephone: (202) 467-6900
Fax: (202) 467-6910
www.wcsr.com

Gregg P. Skall
Direct Dial: (202) 857-4441
Direct Fax: (202) 261-0041
E-mail: GSkall@wcsr.com

May 13, 2010

VIA ELECTRONIC FILING

Ms. Marlene Dortch
Secretary, Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

**Re: Ex Parte Presentation
PS Docket: 08-51**

Dear Ms. Dortch:

Pursuant to Section 1.1206(b) for the Commissions Rules this letter is to inform the Commission that on March 31, 2010 representatives from American Roaming Network met with staff from the Public Safety and Homeland Security Bureau (PSHSB). Representing American Roaming Network was Milton Volz, Steve Williams, Ken Boggs, and the undersigned counsel to the company. PSHSB participants included Thomas Beers, Jeff Cohen and Patrick Donovan.

During the meeting we discussed the comments and reply comments filed by ARN in PS Docket 08-51, and problems presented in mounting a demonstration of the ARN proposed solution to NSI mobile 911 calls. The attached overview was provided to the PSHSB staff.

Please direct any questions to the undersigned.

Sincerely,

A handwritten signature in blue ink, appearing to read "Gregg P. Skall".

Gregg P. Skall



American Roaming Network (ARN) NSI-E911 Call Filtering System

E911 Provider and ARN

American Roaming Network
Ken Boggs, Steve Williams, Gregg Skall and Milton Volz
March 31st, 2010



E911 NSI Call Problem

- ▶ E911 Centers are experiencing high levels of Non-Emergency calls from Non Service Initialized (NSI) Phones
 - >90% of E911 calls from NSI handsets are not legitimate E911 calls
 - Some justifications reported that less than 1% of NSI calls were legitimate.
 - Most of the non-legitimate calls are simple user error and not from malicious intent.
 - PSAPs are vulnerable to “denial of service” attacks

ARN is uniquely positioned



- ▶ ARN is uniquely positioned to provide a reduction in non-legitimate NSI call volume without affecting public safety
 - ARN already handles more than 16 million call per month from NSI handsets and is the sole source processor of NSI calls in the US for CDMA phones, est. 1991.
 - ARN has developed a unique solution that:
 - Can be implemented immediately with no modification to handset or E911 systems
 - Provides a method for the calling party to complete urgent calls via alternate routing/billing methods (Per FCC mandate for “Manual Roaming” [CFR 47 20.12c](#))
 - Provides a method for screened E911 calls to connect to the correct PSAP.

ARN's NSI Experience



- ▶ ARN is uniquely positioned to provide solutions
 - ARN is integrated with most of the wireless carriers in the US on an exclusive basis.
 - Has agreements with wireless carriers allowing ARN to complete non-emergency NSI calls. ARN remits a portion of payments to the wireless carrier.
 - Already handles more than half a million calls per day from NSI callers dialing a North American phone numbers
 - Of the 500,000 calls per day that ARN receives, we complete about 10,000 calls. In effect, we filter 98% of all calls with a 2% completion ratio which is similar to E911 statistics.
 - ARN has registered users using NSI phones.

E911 NSI Scale of Problem



- There are 8.8 million mobile E911 calls per month
- Approx 9% are from NSI mobiles or 800,000 calls per month
 - More than 90% of all NSI E911 calls are invalid or bogus
 - Over 720,000 invalid/bogus E911 calls per month come from NSI mobiles

The average E911 Fee imposed on every mobile is \$.72 per month

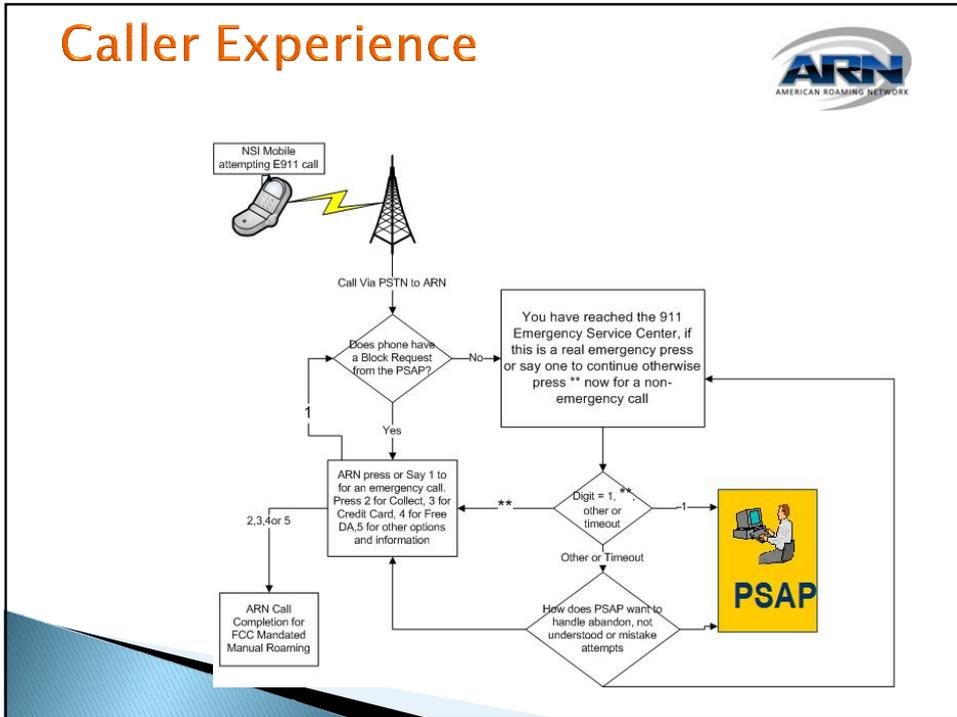
- The total mobile E911 fees collected is \$199M/month
- Therefore \$22.43 in fees are collected per mobile E911 call
- To summarize, the total cost of invalid/bogus NSI 911 calls is greater than \$193M/yr and growing
 - Field dispatch costs are not included in the above calculations but we estimate that an equal amount of cost is expended from invalid/bogus NSI calls

E911 NSI Vulnerabilities



- E911 system is vulnerable to “Denial of Service” attacks
 - Unable to respond effectively to most attacks
 - Unable to isolate originating location of attack
 - Risk of total system blockage/overload
- New devices are entering the market place that will appear to the PSAP as a NSI mobiles. Some of these devices could be remotely controlled from anywhere in the World to create denial of service attack.
- ARN’s proposed solution, with it’s regional gateways, will create a place in the telephone network outside of the current E911 system where this type of attack could be quickly mitigated and centrally or regionally controlled down to the PSAP level.

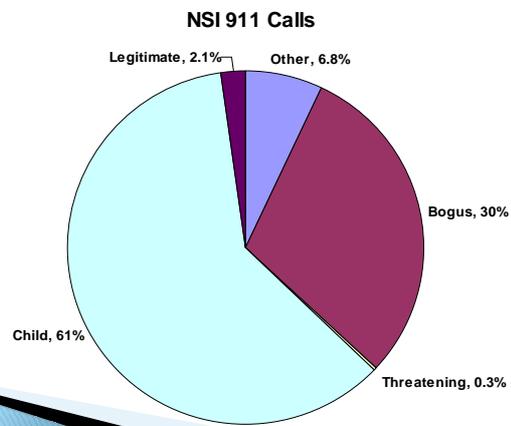
Caller Experience



Effectiveness of Filtering



- Filtering can be designed to target illegitimate calls without significantly delaying legitimate calls
- Filters can be set to block denial of service attacks



Customizable Filtering and Blocking



- The call prompts and filter decisions are controlled depending on State or PSAP requirements
- Filtering can be set on a mobile to mobile basis.
 - Specific callers or groups of callers could be given custom treatment, transferred and/or blocked from 911 access
 - A PSAP may want to play unique prompts to certain offenders to try to persuade the caller to stop calling.
 - There are some limitations depending on the ability to identify a specific mobile
- Filtering decisions can be changed as conditions change
 - In a 911 overload condition, NSI calls can be throttled or blocked altogether

Customizable Filtering and Blocking



- ARN has experience in registering NSI mobiles to use ARN's Manual Roaming Service
- This same process can be used as a filter for E911 NSI Callers
 - Registered caller information can be passed to the PSAP
 - Registered Callers can hear custom prompts
 - Unregistered callers can be given custom treatment or be blocked
- Registration process can happen
 - On ARN's service via IVR on NSI Manual Roaming Calls
 - On E911 NSI Calls via IVR menu
- Would the PSAPs want to charge a monthly or per call fee to registered NSI devices?

Filtering, Blocking and Reporting



- ARN can collect a call back number for the NSI Mobile
 - Call back number can be assigned at registration or
 - during E911 call.
 - The call back number can be optional or required
- ARN's Manual Roaming and NSI E911 call records can be consolidated to compare to help identify offending callers. We assume that some offending NSI callers dialing 911 are attempting and/or completing calls to friends and family on ARN's network. We propose to compare these records to identify offenders.

Customizable Filtering and Blocking



	Country	State	NPA	PSAP	None
Block NSI Attempts By					x
Allow NSI Attempts By					
Filter Options by PSAP	Quantity	All			
Simultaneous Calls allowed	5				
Registration of NSI mobile	Required	Optional	Not		
Call Back Number of NSI Caller	x	x	Used		
Prompt Timeout 1st	PSAP	Main	ARN		
Prompt Timeout 2nd	x	Menu			
Invalid option selection 1st		x			
Invalid option selection 2nd	x				
Send Black List ANI to	PSAP	Main	ARN	Registration	
Registered Black List treatment	N/A	Menu	x	Req	
	x			x	



FCC Notice of Inquiry (PS Docket 08-51)

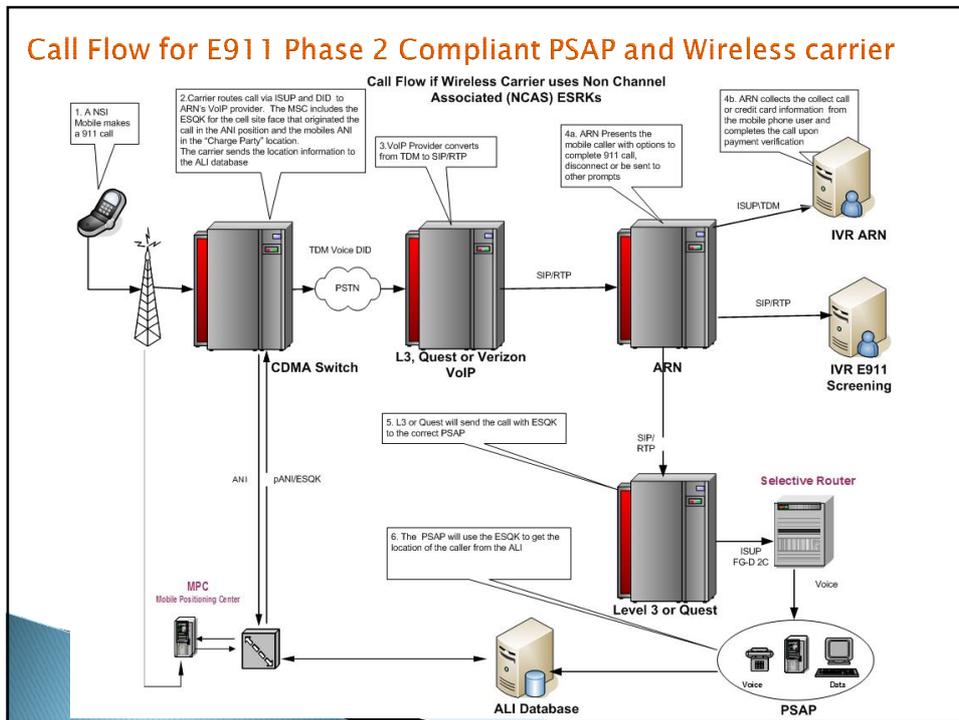
- ▶ Call-Forwarding requirements and Carriers Blocking Options for Non-Initialized phones
 - In 2002 the FCC released its second Report and Order addressing NSI issues. In this reports it clarified that
 - Does not preclude “carriers from blocking fraudulent 911 from non-service initialized phones pursuant to applicable state and local law enforcement procedures”
 - The clarification above does not go far enough to allow for Filtering of all NSI calls. How can this be resolved?



Technical detail

- ▶ The following slide shows the network elements and call flow involved NSI calls to reach the screening IVR and be redirected back to the correct E911 Jurisdiction.
 - This slide represents just one of the possible solutions. Many other variants can be deployed to achieve call screening goals.
 - The slide assumes the 911 center and Wireless carrier are phase two compliant and the wireless carrier can and will separate NSI calls from normal calls.

Call Flow for E911 Phase 2 Compliant PSAP and Wireless carrier



E911 Filtering Test Partners



• In order for a test to proceed, ARN requires cooperation from a Wireless Carrier, a PSAP entity, the PSAPs infrastructure provider and the Wireless Carrier's infrastructure provider. The team working with ARN consists of:

- Wireless Carrier
 - Revol Wireless
- Wireless Switch Vendor of Revol
 - Nortel
- PSAP
 - Indiana Wireless E911 Board- Kenneth Lowden
- PSAP's infrastructure provider
 - INdigital

Test Design Concepts



- Prove the design concepts:
 - Separation of the NSI E911 calls from the Normal E911 calls by the Mobile Switching Center
 - Redirection of the screened calls back to the PSAP using the ESRK
 - Measure reduction in fraudulent calls
 - Calculate all of the cost to provide the service in a wide scale deployment
 - Identify enhancements

Issues That Delay the Testing



- The test will cost as much as \$450,000. Approximately \$300,000 will go to Nortel to develop a feature to split the NSI calls from the Non-NSI calls
- In order to secure funds for the test we must we first have a reasonable expectation that a successful test will result in a wide scale deployment.
- Issues that can prevent wide scale deployment:
 - Lack of regulatory support
 - Concerns of liability for handling of E911 calls
 - Acceptance by industry groups of the solution
- Without the above conditions being met we will need Public Funding for the test to go forward

Next Steps



- Gain regulatory favor for ARN's filtering approach
 - Find and research objections
- Review technical capabilities and limitations
- Review Legal and liability Issues
 - Currently varies by state