

Understanding Carrier IQ Technology

What Carrier IQ Does and Does Not Do

December 12th 2011

Introduction

Following recent public discussions and questions on the use and deployment of Carrier IQ, this document is designed to provide answers and share how our software is deployed and used.

We want to thank Trevor Eckhart for sharing his findings with us through a working session that helped us to identify some of the issues highlighted in this report. We also want to thank security researcher Dan Rosenberg for his thorough analysis and industry recommendations and the cooperation of Network Operators in assisting our investigations.

In this document, we want to let consumers to know exactly what it is that our software does, the security measures we have in place, and our commitment through our software design and processes to protecting consumers' privacy while improving consumers' experience.

This document outlines the following:

- Details of the Carrier IQ solution and how it is deployed
- How the Carrier IQ software – “IQ Agent” - is loaded on mobile devices
- What information is available to Mobile Network Operators from devices
- How data from mobile devices may be used by Carrier IQ's customers
- How consumer data is protected through this process

Section 1: Carrier IQ Solution Background

Carrier IQ was formed in 2005 to provide answers to some very simple but critical questions that mobile telephone companies – “Network Operators” – have: what is the network service quality consumers experience when they use a mobile phone on our network and how do we make it better? Put another way, what actually causes dropped calls, reception issues and the like? Due to the nature of mobile networks, one efficient and effective way to answer these questions is to implement diagnostic software within the phone that could summarize how the phone and services were performing on the network. This software could then automatically relay this information to the Network Operator who could take action to solve the problems and ultimately improve the consumer’s experience. This has been our mission since the formation of the company.

Carrier IQ believes that having diagnostic data delivered from the mobile device is a far superior solution than traditional methods of analysis -- using statistics gathered through consumer surveys, sending trucks around a city or the countryside to capture cellular performance (called “drive testing”), or endlessly questioning a consumer about the details and circumstances each time they call the support center with a problem.

In building a solution capable of scaling to millions of subscribers, we understand that having an effective solution requires that the software gather only the critical diagnostic information and do so in a manner that protects consumers’ information. From a business perspective, using the least amount of data possible reduces costs in providing the service (less storage facilities, less data to analyze).

Carrier IQ has built software that allows Network Operators to better understand how mobile devices interact with and perform on their network. Today our technology is used in two specific ways: network management and customer care.

Network Management

Carrier IQ software provides Network Operators with diagnostic services that help them identify how their network, and devices on their network, are performing. This can include: data on when and where calls fail; where customers have problems accessing the network; the reliability and battery performance of their make and model of device; and the interaction of the mobile network with your mobile device – known as network signaling traffic. This information can be aggregated to provide performance scorecards and heat maps by market or city, or by type of device. (Example screen shots from our applications can be found in Section 3.)

Customer Care

The diagnostic information from the phone can also be used to assist individual users who are experiencing problems with their device or with the network. For example, let's look at a situation where a consumer makes a call to the Network Operator's customer service center. In order to respond, the customer service center needs the device data so the Carrier IQ software automatically passes the hardware serial number and the subscriber serial number (e.g. IMEI/IMSI) to the Network Operator who can then match to their customer records. Carrier IQ provides the Network Operator with a summary of the user's experience which can include network performance, battery life, ability and speed to access a website (also known as "throughput"), and the usage, performance and stability of an application. (Screen shots from these applications are in Section 3.) Below are some example questions and example answers that this solution provides:

Q. "Why is my battery only lasting 3 hours and my phone keeps crashing?"

A. Because you have loaded a new application *abcxyz* and this is draining the battery quickly and making your phone unstable.

Q. "Why does my phone drop calls when I drive on Interstate 80?"

A. It looks like you were dropping calls between exit 34 and exit 35 and we are upgrading our towers to improve performance at that section of the highway.

Section 2: Carrier IQ Software on the Mobile Device

The Carrier IQ software installed on the mobile device is called the IQ Agent. The IQ Agent is the first stage in the Network Operator's analytics pipeline and is responsible for identifying, storing and forwarding diagnostic measurements and data from the handset and the network required to solve network and consumer issues. The IQ Agent has been implemented on feature phones, smart phones, data modems and tablets.

We designed the IQ Agent with the objective of not impacting the user's experience (by draining battery, slowing the device or consuming memory and CPU resources). Handset manufacturers and Network Operators take our software through a formal device certification process to ensure that each implementation meets this requirement.

In processing and analyzing performance from millions of devices for a Network Operator, operational efficiency requires that the smallest possible amount of information be gathered to avoid the cost and expense of processing data that does not solve a network management or customer care problem. The IQ Agent is able to summarize the diagnostic information before it is uploaded to the network, greatly reducing the amount of data transmitted and subsequent data processing costs. The bottom line: The less data gathered to detect and resolve problems, the more cost-effective our solution becomes.

In typical deployments, the IQ Agent uploads diagnostic data once per day, at a time when the device is not being used. This upload, which averages about 200 kilobytes, contains a summary of network and device performance since the last upload, typically 24 hours. Network Operators who are Carrier IQ customers do not charge consumers for this upload nor does it show up as usage of consumer data plans.

The frequency and type of information uploaded is defined by the Network Operator and is called a *profile*. The profile enables our customers to define custom rules that gather the measurements they need to answer a specific performance question. These individual measurements on a device, such as signal strength, are called *metrics*. Each mobile network is different from the others. In order to serve all of those varying needs, Carrier IQ created software that allows Network Operators to create a subset of these metrics (a profile) tailored to solve their individual network requirements.

For example, if a Network Operator is interested in understanding the cause of dropped calls, a specific profile can be created to address this issue. That profile is passed to devices loaded with the IQ Agent instructing the devices to provide the Network Operator with *metrics* for dropped-call events. The profile then gathers the associated signaling messages, location, radio conditions and any other essential measurements leading up to the call termination, thus eliminating non-essential data, such as successful call events. More details on *profiles* are described later in this section.

Before Carrier IQ diagnostics can be gathered from a mobile device, this IQ Agent must be installed. There are three ways in which Carrier IQ's customers install the IQ Agent, pre-load, aftermarket and embedded. These methods are described below:

Preload IQ Agent

In this method, Carrier IQ provides its customers with a complete version of the IQ Agent that the device manufacturer installs on the device prior to shipment on the instruction of a Network Operator. This version of IQ Agent does not require integration by a device manufacturer and diagnostics are gathered by the IQ Agent through publicly available operating system APIs. In this implementation, Carrier IQ's software has access to no more data than any other application on a device. Exhibit B provides a list of the types of metrics available in this mode, but the main difference between pre-load and embedded is that the radio diagnostic data – detailed RF measurements or layer-3 protocol messages sent between the tower and the mobile device – are not available for analysis with the pre-load version.

This version of the IQ Agent cannot typically be deleted by an end user but only gathers and forwards *metrics* from the device if it is enabled with a *profile* which is described later in this section.

After-market downloadable IQ Agent

The IQ Agent is also available as a download such that it may be installed by consumers after they have purchased the device. In this model, a mobile device user would download the IQ Agent on instruction from Carrier IQ's customer – typically a Network Operator. The metrics available to the downloaded IQ Agent are the same as the pre-load agent (see Exhibit B). This is the least-used deployment model as Network Operators typically employ pre-load or embedded versions.

As the application is installed by the end user, just like any other after-market mobile application, it may be deleted by the consumer. As with other versions of the IQ Agent, the software only gathers analytics if activated with a profile.

Embedded IQ Agent

In this method, handset manufacturers install the IQ Agent configured to collect metrics specific to that device and to Network Operator requirements. Unlike the pre-load and downloadable version of the agent, this method of integration incrementally provides the IQ Agent software with metrics that measure radio signaling messages between the handset and radio towers. (See Exhibit B for list of the types of metrics available with the embedded agent.) Network Operators typically prefer the embedded version of the software as it provides the most comprehensive diagnostic set. This embedded information is used to understand which control signals are passed between the mobile device and the handset and is used to resolve why a problem might be occurring (such as a dropped call).

To install the software and report the correct Network Operator defined metrics-set, Carrier IQ provides the handset manufacturers with a porting guide and a metric requirements specification. The guide and the specifications enable the handset manufacturer to write a software interface to pass the necessary *metrics* from the handset to the IQ Agent using the Carrier IQ-specific Application Programming Interface (API) described in the porting guide. This Carrier IQ specific API is the only mechanism by which IQ Agent receives *metrics* from the mobile device operating system.

Activating & Deactivating Embedded IQ Agent

Network Operators and handset manufacturers determine whether and how they deploy Carrier IQ software and what *metrics* that software will gather and forward to the Network Operator.

The IQ Agent only gathers and forwards *metrics* from the device if it is enabled with a *profile* which is described in more detail later in this section. An embedded version of the IQ Agent cannot be deleted by consumers through any method provided by Carrier IQ.

Profiles

While each mobile device containing Carrier IQ software can be implemented with a comprehensive list of analytics capabilities (see Exhibit A), **what is actually gathered by a Network Operator is based on their business requirements and the agreements they form with their consumers on data collection.**

The profile defines which of the available metrics are to be gathered and provides instructions on how to pre-process the data prior to uploading. For example, the profile may request that the IQ Agent summarize broadband throughput for the previous twenty-four hours.

Each profile will contain the following information:

- 1) Should information be collected in anonymous mode or with the hardware serial number and the subscriber serial number being used (e.g. IMEI & IMSI)?
- 2) The frequency of *metrics* uploads and instructions on what to do if the user is roaming or not on the network
- 3) The specific *metrics* from which to gather data
- 4) Instructions for pre-processing of metrics to create summary information

The profiles are written by Carrier IQ based on information requested by our customers (predominantly Network Operators). Each Network Operator typically has multiple profiles that are created to provide answers to specific problems.

A new profile can be downloaded to a mobile device when it periodically checks-in with the network server. After receiving the new profile from the network server, the device will begin gathering the metrics and pre-processing according to these instructions.

Recently Discussed Issues

In this section we discuss a number of critical allegations and questions that have been raised through the last weeks. Our goal is to increase transparency on these issues and answer specific questions that have been raised about Carrier IQ's software.

Android System Log files

In Trevor Eckhart's video, an Android-based HTC device is shown writing location, keylog and SMS information to an Android log file in clear (human readable) text. A log file is a human-readable file which typically contains device events and important information related to the operation of a device.

We cannot comment on all handset manufacturer implementations of Android. **Our investigation of Trevor Eckhart's video indicates that location, key presses, SMS and other information appears in log files as a result of debug messages from pre-production handset manufacturer software. Specifically it appears that the handset manufacturer software's debug capabilities remained "switched on" in devices sold to consumers.**

As discussed, in the embedded deployment model, the Carrier IQ API is the only method by which *metrics* are passed from the device operating system to the IQ Agent. **The IQ Agent does not use the Android log files to acquire or output metrics.**

Various parties in the industry, including security consultants such as Dan Rosenberg, have recommended that handset manufacturers switch off debug messages containing personal information to prevent them being written into log files. In addition, Carrier IQ is working with handset manufacturers and Network Operators to suggest changes to the certification process for new devices to prevent similar problems from occurring again.

Layer 3 Signaling Traffic Metrics with Embedded IQ Agent Versions

Over the course of the past week, as Carrier IQ conducted extensive reviews with the Network Operators, Carrier IQ has discovered an unintended bug in a diagnostic profile to measure radio-network-to-mobile device signaling. This diagnostic profile is used to gather network conditions during voice calls to determine why they fail. Using these profiles, the IQ Agent collects "layer 3" signaling traffic between the mobile device and radio tower, to help the Network Operator determine, for example, why a call might be dropped or which radio towers are communicating with a device during a voice call. **Carrier IQ has discovered that, due to this bug, in some unique circumstances, such as a when a user receives an SMS during a call, or during a simultaneous data session, SMS messages may have unintentionally been included in the layer 3 signaling traffic that is collected by the IQ Agent. These messages were encoded and embedded in layer 3 signaling traffic and are not human readable.**

Carrier IQ does not decode or process any SMS messages that may have been embedded in the layer 3 signaling traffic collected in these instances. While the entire layer 3 signaling traffic that was captured

was provided to the Network Operators, either to their own data centers or to the servers hosted for them in Carrier IQ's data centers, the content of any encoded and embedded SMS is not shown or available to Carrier IQ, its Network Operator customers or any other party. For Network Operators to view the specific content of SMS messages, Carrier IQ would need to write additional software, which has never been done. **No multi-media messages (MMS), email, web, applications, photos, voice or video (or any content using the IP protocol) has been captured** as a result of this profile bug, as only SMS traffic is embedded in layer 3 signaling messages to deliver SMSs to/from devices.

Carrier IQ customers who have deployed the embedded version of the IQ Agent have been informed of this bug, and Carrier IQ has worked with customers to fix it and ensure that this information is no longer captured. Only embedded versions of our software are affected by this bug.

Phone Numbers

Our customers – Network Operators – record phone numbers as a consequence of generating billing records. Also, in the process of gathering metrics on the performance of these calls, the IQ Agent will record the same phone numbers dialed and received for the purpose of diagnosing and maintaining their networks. If selected through the profile, this functionality allows a Network Operator to understand both ends of a problem. For example, Carrier IQ's software allows the Network Operator to determine in a dropped call situation which consumer's phone had the problem that caused the drop.

Web URLs

The embedded version of IQ Agent *metrics* allows for the collection of URLs if requested in a *profile*. These can be collected together with performance metrics so that Network Operators can measure consumer experience for specific web sites. For example, if a Network Operator were experiencing issues with traffic destined for a heavily used web site, this diagnostic information could help determine user impact and help the Network Operator manage resources. The profile specified by the Network Operator and loaded on the device dictates if this information is actually gathered. **The IQ Agent cannot read or copy the content of a website.**

Local Storage of Information and Upload

The *metrics* gathered by the IQ Agent are held in a secure temporary location on the device in a form that cannot be read without specifically designed tools and is never in human readable format.

The length of time this information is held on the device before upload is based on the *profile* but is typically 24 hours.

When it is time to upload the diagnostic data, the mobile device will request a secure encrypted channel to the network server and transmit the diagnostics from the device to the network server.

Collection of Keystrokes & SMS as seen in Trevor Eckhart's Video

Under normal circumstances, the IQ Agent checks-in to the network server and transmits the diagnostics securely against the schedule defined in the profile. There are two additional methods which can cause the agent to check-in:

- 1) A specific numeric key code can be entered by the user of the mobile device through the dialer
- 2) The collector may send the device an SMS which contains a request to commence check-in

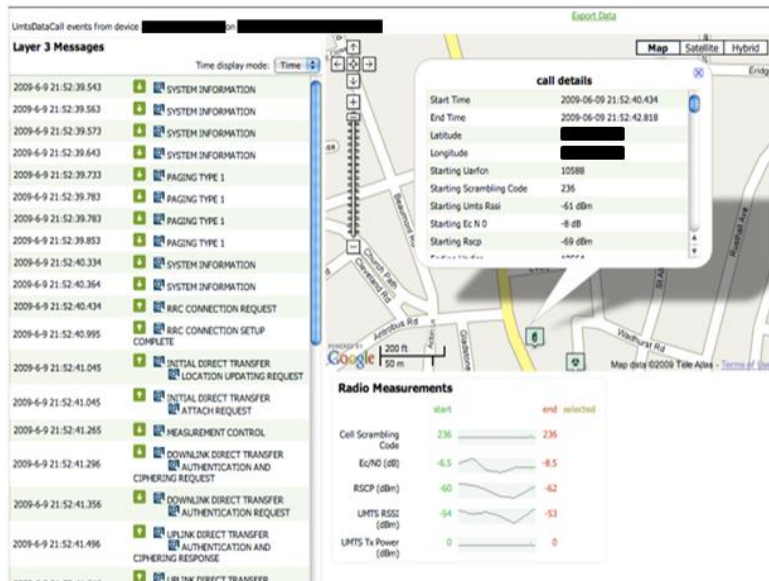
These two mechanisms require Carrier IQ Agent software to recognize specific codes entered into the keypad or specific SMS messages received. **These mechanisms do not provide a method for Carrier IQ to capture keystrokes or the content of SMS.**

As discussed previously, what was shown in the video demonstrated keystrokes and SMS being written to Android log files, not stored or transmitted by the IQ Agent.

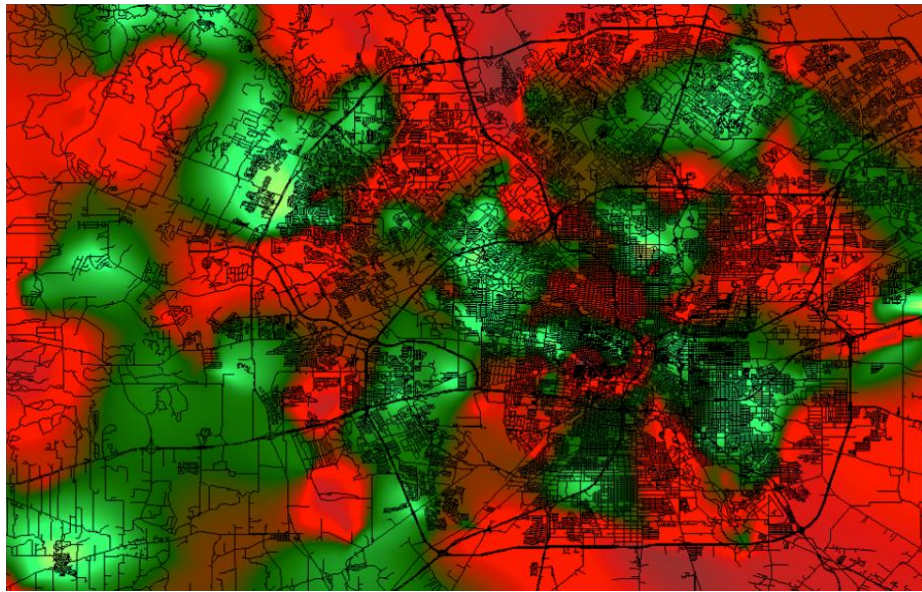
Section 3: Mobile Service Intelligence Platform (MSIP™)

The Mobile Service Intelligence Platform is a wireless analytics platform that enables our Network Operator customers to define and manage the information they receive from the devices and network. The software allows Network Operators to identify groups of devices to participate in different use cases and to process and analyze the resultant measurement data. For example, an Operator may want to determine the interaction of its network with a new high-profile smartphone launch, manage and troubleshoot a new service launch like LTE, reduce roam-at-home occurrences, or perform an investigation into an existing service or device issue. The MSIP also provides reporting and visualization tools that our customers use for network planning (where there should be more towers), optimization (where there may be network congestion because of a high concentration of users) and customer care.

The tool we use for diagnosing network issues is called IQ Insight and provides details on the location of events such as dropped calls or no service areas. A network technician can drill down from a map view to understand exactly what happened at the time of a failure and use this information to fix issues.



Screenshot: Signaling messages

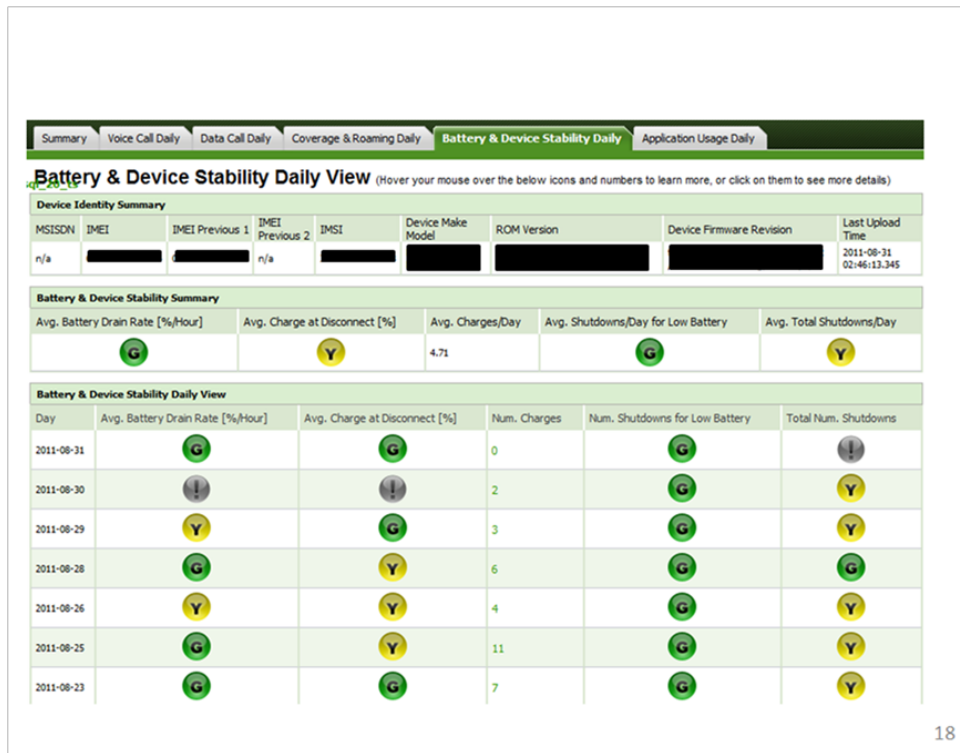


Screenshot: Heat map of a geographic area showing signal strength

In the customer care example, Carrier IQ provides a customer experience dashboard to operators which provides quality of service information experienced by a specific consumer. Again, the Network Operator’s customer service agent is able to drill-down into specific details of what may have caused a specific problem, allowing them to provide more effective and efficient service to the consumer.

IQ Insight - Device Analyzer OTA													
		Select IQGroup		Analytics		My Account		IQGroup Management		User Management			
		Summary		Voice Call		Data Call		Coverage & Roaming		Battery & Device Stability		Application Usage	
Selected IQGroup Customer_Care		Customer Experience Dashboard											
Dashboards		Analysis Criteria											
Device Quality		IMEI: [REDACTED]		IMSI: [REDACTED]		Last 30 Days		2011-12-08		Refresh			
Coverage Analysis		Device Identity Summary											
Customer Experience		MSISDN	IMEI	IMEI Previous 1	IMEI Previous 2	IMSI	Device Make Model	ROM Version	Device Firmware Revision	Last Upload Time			
Reports		[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	2011-11-27 01:28:59.926			
Analytics		Overall Score											
Tools		Voice Experience Summary	Data Experience Summary	% Time with No Signal	Avg. Battery Drain Rate [%/Hour]		% Application Failures						
Dev Tools		G	Y	G	Y		G						
Help		Daily Summary											
Data Attributes		Date	Voice Experience Summary	Data Experience Summary	% Time with No Signal	Avg. Battery Drain Rate [%/Hour]		% Application Failures					
User Guide		2011-11-26	Y	↓	G	G		G					
		2011-11-25	G	Y	G	G		G					
		2011-11-24	Y	Y	G	Y		G					
		2011-11-23	G	Y	G	Y		G					
		2011-11-22	G	Y	G	Y		G					
		2011-11-21	G	↓	G	Y		G					

Screenshot: Experience summary for a specific consumer



Screenshot: Battery & stability performance for a specific consumer

Location and Security of Data

The location of Carrier IQ MSIP servers varies by customer. Carrier IQ provides a “Software-as-a-Service” model whereby we host the servers on behalf of some customers. In other cases, our customer will host the MSIP system in their data centers. In either case the security of the systems is paramount and our customers audit the protections we place in these systems and facilities. To date we have not experienced any known data breaches. It should also be noted that customer identifying information beyond the hardware and subscriber serial numbers and phone numbers dialed/received is not kept in Carrier IQ deployed systems.

Other uses of Data

Carrier IQ have no rights to the data that is gathered into the MSIP system for any Carrier IQ customer.

Under our customer contracts we are not permitted to analyze, resell or reuse any of the information gathered for our own purposes, or to pass to any third party unless required by law.

Summary

In this document we described the importance of consumer experience data in determining both network and device issues and how this information is actually used to solve problems. Carrier IQ and our customers believe the analytics our software delivers has a direct impact on the operation, maintenance and reliability of networks and the ability of Network Operators to actually understand and solve consumer problems when they call for help.

To summarize this report:

- The source of personal information in Android log files shown by Trevor Eckhart in his video is a result of debug settings remaining in production devices and should be classified as vulnerability. **The IQ Agent software on the mobile device was not responsible for writing log messages containing personal information seen in the video.**
- **Carrier IQ does not acquire or forward the content of multi-media messages (MMS), emails, photos, web pages, audio or video.** A detailed list of what is actually gathered can be found in Exhibit A and Exhibit B.
- **In some unique circumstances described in this document, an unintended bug in a diagnostic profile allowed collection of layer 3 radio messages in which SMS messages may have been embedded.** While the layer 3 signaling data was provided to the Network Operators over whose networks the data was originally sent, they were not decoded or made available in human readable form to Carrier IQ, its customers or any third party. Upon discovering the bug, Carrier IQ and its customers took immediate steps to remedy the bug and Carrier IQ customers are no longer uploading such data.
- A specific numeric key code can be entered by the user to cause the IQ Agent software to commence an upload and the IQ Agent software on the device receives numeric key presses so that it can identify when this key code is entered. **Carrier IQ has never intentionally captured or transmitted keystrokes and is not aware of any circumstances where this has occurred. Carrier IQ is not a keylogger and no customer has asked Carrier IQ to capture key strokes.**
- Network Operators define through profiles which specific diagnostics are actually gathered from a device. Carrier IQ writes profiles for each Network Operator to gather the diagnostic information they require.

We will extend the contents of this document to reflect new questions and issues as they may arise.

Wireless Analytics (Exhibit A)

Carrier IQ offers a comprehensive suite of analytics for wireless network and device performance. The *metrics* collected by the device are used to compute measures and performance indicators that characterize the device and service performance at each layer in the protocol stack providing deep insight into the overall customer experience, good or bad, and facilities to help determine the actual cause for device or network issues. A compendium of the available analytics domains is listed below.

<p>Radio Technologies and Domains</p> <ul style="list-style-type: none"> • EVDO/CDMA (Rev 0 and Rev A) • GSM/UMTS/HSPA • LTE/CSFB • Idle mode coverage and roaming <p>Circuit-Switched Voice Services</p> <ul style="list-style-type: none"> • Call attempts (GSM/WCDMA) • Call establishment success/failure • Call setup latency • Handover performance • Call-end cause analytics • Root cause (coverage, pilots) • Device cross domain • Active mode roaming <p>UMTS and CDMA/EVDO Data</p> <ul style="list-style-type: none"> • Mobility & session management • RLC and PHY throughputs and data volume • Setup latency • RRC performance • 2G/3G/4G hand down • Device cross domain 	<p>Application, Battery, UI</p> <ul style="list-style-type: none"> • App context changes (focus/background) • Charge cycles • Battery charge level and drain • Screen touch events • Backlight and CPU (Android) <p>IP and IP Services</p> <ul style="list-style-type: none"> • Application protocol throughput, latency • HTTP, FTP, IMS • IP throughput, latency, packet Loss <p>Device Stability and Device Status</p> <ul style="list-style-type: none"> • Device configuration • Device crashes • Power on and power off events • Memory/flash status
--	---

Wireless Metrics (Exhibit B)

This exhibit describes individual items – *metrics* – that can be examined on a device. This list shows the maximum number of available metrics and is updated on a quarterly basis. Not all of the metrics shown are implemented on all devices for all Operators. What is actually gathered from a device is defined by a profile. A profile requests the collection of a sub-set of available metrics. The profile may upload metrics directly, or allow metrics to be summarized on a device prior to upload. As discussed in this document, there are three deployment models for Carrier IQ software. The table shows both embedded and non-embedded. The non-embedded column shows metrics for both pre-installed and aftermarket download.

Metric	Embedded	Non-Embedded	Metric	Embedded	Non-Embedded
AL34 - Browser Page Fetch Start	✓		DO44 - EVDO Layer 3 - TrafficChannelAssignment	✓	
AL35 - Browser Page Fetch Event	✓		DO45 - EVDO Layer 3 - FixedModeEnable	✓	
AL36 - Browser Page Fetch End	✓		DO46 - EVDO Layer 3 - BroadcastReverseRateLimit	✓	
DL04 - 1xRTT Access Channel Message	✓		DO47 - EVDO Layer 3 - UnicastReverseRateLimit	✓	
DL05 - 1xRTT Reverse Traffic Channel Message	✓		DO48 - EVDO Connection Attempt Success	✓	
DL06 - 1xRTT Sync Channel Message	✓		DO49 - EVDO Connection Attempt Failure	✓	
DL07 - Layer 3 Paging Channel Message	✓		DO4A - EVDO FTC Stats Rev0 Condensed	✓	
DL08 - 1xRTT Forward Traffic Channel Message	✓		DO4B - EVDO FTC Stats RevA Condensed	✓	
DO31 - EVDO Layer 3 - Control Channel Directed	✓		DO4C - EVDO RTC Stats RevA Condensed	✓	
DO32 - EVDO Layer 3 - Access Channel	✓		DO4D - EVDO Connected State Open	✓	
DO33 - EVDO Layer 3 - Forward Traffic Channel	✓		DO4E - EVDO Connected State Inactive	✓	
DO34 - EVDO Layer 3 - Reverse Traffic Channel	✓		DO4F - EVDO Sector ID	✓	
DO35 - EVDO Layer 3 - Control Channel Broadcast	✓		DO4G - EVDO RF Receive Set	✓	
DO36 - EVDO FTC Stats Rev0	✓		DO4H - EVDO RF Transmit Set	✓	
DO37 - EVDO RTC Stats Rev0	✓		DO4I - EVDO QuickConfig Message	✓	
DO38 - EVDO FTC Stats RevA Single-User	✓		DO4J - EVDO Pilot Sets	✓	
DO39 - EVDO RTC Stats RevA	✓		FP01 - FTP Command	✓	
DO3B - EVDO RF Set	✓		FP02 - FTP Reply	✓	
DO3D - EVDO DRC Cover	✓		FP03 - FTP Data Packet Event	✓	
DO3E - EVDO Pilot Sets	✓		FP04 - FTP Data Transfer Start	✓	
DO3F - EVDO Connection Attempt	✓		FP05 - FTP Data Transfer End	✓	
DO3G - EVDO Connection Release	✓		GS01 - GSM/UMTS Circuit Switched Call Start	✓	✓
DO3H - EVDO State	✓		GS02 - GSM/UMTS Circuit Switched Call State Transition	✓	✓
DO3N - EVDO RevA Multi-User Packets User Stats	✓		GS03 - GSM/UMTS Circuit Switched Call End	✓	✓
DO3O - EVDO Access Attempt	✓		GS15 - PDP Context Activation	✓	✓
DO3P - EVDO Session Attempt	✓		GS18 - PDP Context End	✓	✓
DO3Q - EVDO Active Set Pilot	✓		GS19 - PDP Context Request	✓	✓
DO3R - EVDO Multi-RLP Fwd Stats	✓		GS30 - GSM/GPRS/EDGE Layer 3 Downlink Message	✓	
DO3S - EVDO Multi-RLP Rev Stats	✓		GS31 - GSM/GPRS/EDGE Layer 3 Uplink Message	✓	
DO3T - EVDO Enhanced MRLP Fwd Stats	✓		GS34 - UMTS/HSPA Layer 3 Downlink Message	✓	
DO3U - EVDO Enhanced MRLP Rev Stats	✓		GS35 - UMTS/HSPA Layer 3 Uplink Message	✓	
DO3V - Extended QoS State	✓		GS46 - GSM/GPRS/UMTS Network Info	✓	✓
DO3W - Extended QoS Requested	✓		GS47 - Service State	✓	✓
DO3X - Extended QoS Granted	✓		GS54 - Handover Begin	✓	
DO3Y - Extended QoS Modified	✓		GS55 - Handover End	✓	
DO40 - Booster Pack Version	✓		GS57 - Cell Change Begin	✓	
DO41 - EVDO Layer 3 - UATIAssignment	✓		GS58 - Cell Change End	✓	
DO42 - EVDO Layer 3 - SectorParameters	✓		GS66 - Active Set Update	✓	
DO43 - EVDO Layer 3 - QuickConfig	✓				

Metric	Embedded	Non-Embedded
GS6D - Multi-RAB State	✓	
GS6E - Radio Mode	✓	
GS6F - Compressed Mode State	✓	
GS81 - GPRS/EDGE RLC Statistics	✓	
GS83 - HSPA Statistics	✓	
GS84 - UMTS/HSPA RLC Statistics	✓	
GS86 - RLC Reset	✓	
GS88 - HSDPA Evolved Statistics	✓	
HT01 - HTTP Request Start	✓	
HT02 - HTTP Request Header	✓	
HT03 - HTTP Request Finish	✓	
HT04 - HTTP Response Start	✓	
HT05 - HTTP Response Header	✓	
HT06 - HTTP Response Finish	✓	
HT07 - HTTP MIME Type	✓	
HW03 - Battery Event	✓	
HW04 - Reverse Logistics	✓	
HW10 - Battery Information	✓	
HW11 - Battery State	✓	✓
HW12 - Device Reset/Reboot	✓	
HW13 - Binary Data	✓	
IP01 - IP Interface Creation	✓	
IP02 - IP Flow End Statistics	✓	
IP03 - IP Flow Status Statistics	✓	
IP04 - DNS Lookup Attempt	✓	
IP05 - DNS Lookup Resolution	✓	
IPTX - IP Packet Transmission	✓	
IPRX - IP Packet Reception	✓	
IPVR - IP Booster Pack Version	✓	
UPTR - Upload Triggered	✓	✓
LC01 - Provide Pilot Phase Measurement	✓	
LC02 - OTA System Parameters for Location	✓	

Metric	Embedded	Non-Embedded
LC05 - Pilot Phase Measurement (packed)	✓	
LC07 - Last X OTA Params Seen	✓	
LC11 - Standard Set of dynamic RF info submitted during LC05	✓	
LC12 - Active, Candidate, Neighbor Set during LC05 report	✓	
LC18 - GPS Location	✓	✓
LC30 - Non-GPS Location	✓	
LT01 - E-UTRA RRC Message	✓	
LT02 - E-UTRA NAS Message	✓	
LT03 - E-UTRA Measurement Report	✓	
LT04 - E-UTRA Inter-RAT Measurement Report	✓	
LT05 - E-UTRA Neighbor List	✓	
LT06 - E-UTRA RRC State	✓	
LT07 - E-UTRA MAC Control State	✓	
LT08 - E-UTRA MAC Random Access Attempt	✓	
LT09 - E-UTRA RLC Data Transfer Report	✓	
LT10 - E-UTRA EPS Bearer Context Status	✓	
LT11 - E-UTRA EPS Bearer QoS	✓	
LT12 - E-UTRA PUSCH Transmission Status	✓	
LT13 - E-UTRA Radio Link Sync Status	✓	
MG01 - SMS Sending Start	✓	
MG02 - SMS Sending End	✓	
MG03 - SMS Received	✓	
MG11 - MMS Sending Start	✓	
MG12 - MMS Sending End	✓	
MG14 - MMS Retrieval State	✓	
MG15 - MMS Retrieval End	✓	
MP01 - Media Session Start	✓	
MP02 - Media Session Event	✓	
MP03 - Media Session End	✓	
MP04 - Media Channel Request	✓	
MP05 - Media Channel Result	✓	
NT07 - IP State	✓	
NT08 - IP Session Start	✓	
NT09 - IP Session End	✓	
NT1C - Interface Events	✓	
OS07 - Memory Status	✓	✓
OS08 - File System Summary	✓	✓
QU01 - Survey Start	✓	✓

Metric	Embedded	Non-Embedded
QU03 - Survey Question and Answer	✓	✓
QU04 - Survey Question and Answer	✓	✓
QU05 - Survey End	✓	✓
DO3M - EVDO Roaming Status	✓	
PP01 - Send Buffer Event	✓	
PP02 - Receive Buffer Event	✓	
QC01 - HPPTT Alert Notice	✓	
QC02 - HPPTT Call Attempt	✓	
QC03 - HPPTT Call Completion	✓	
QC04 - HPPTT Call Termination	✓	
QC05 - HPPTT Call Event	✓	
QC06 - HPPTT Application Event	✓	
QC07 - HPPTT Error Display	✓	
QC08 - HPPTT Button Pressed	✓	
QC09 - HPPTT Settings	✓	
QC40 - Booster Pack Version	✓	
QC41 - HPPTT Conference Request (Booster Metrics Pack HPPTT)	✓	
QC42 - HPPTT Conference Status Change	✓	
QC43 - HPPTT Conference End	✓	
QC44 - HPPTT Floor Event	✓	
QC45 - HPPTT Local Floor Grant	✓	
QC46 - HPPTT Floor Grant	✓	
QC47 - HPPTT Floor Release	✓	
QC48 - HPPTT Local Floor Grant Failure	✓	
RF02 - Channel Frequency	✓	
RF04 - SID	✓	
RF05 - NID	✓	
RF12 - Active, Candidate, Neighbor Set	✓	
RF1A - CDMA Roaming Status	✓	
RF20 - RF Power Information	✓	
RF21 - Frame Error Rate	✓	
RF51 - GSM/GPRS/EDGE RF Serving Cell Info	✓	
RF52 - GSM RF Dedicated Set Info	✓	
RF53 - GSM Neighbor Measurements	✓	
RF54 - GPRS/EDGE Link Quality Info	✓	
RF55 - Signal Strength	✓	✓
RF60 - UMTS/HSPA RF Info	✓	

Metric	Embedded	Non-Embedded
RF61 - UMTS/HSPA Active and Monitored Set Info	✓	
RF62 - UMTS/HSPA Inter-RAT Neighbor Measurements	✓	
RF63 - UMTS/HSPA Transport Channel Info	✓	
RF64 - UMTS/HSPA Radio Link Sync Status	✓	
TP01 - TCP Connection Attempt	✓	
TP02 - TCP Connection State	✓	
TP03 - TCP Connection Status - Queried	✓	
TP04 - TCP Connection Status - Changed	✓	
TP05 - TCP Connection Closed	✓	
TP06 - TCP Connection Result	✓	
TP07 - TCP Window Statistics	✓	
SS10 - Mobile Subscriber Number	✓	✓
SS18 - Handset Model	✓	✓
SS1A - Hardware Serial Number	✓	✓
SS1B - Mobile Subscriber Identification	✓	✓
SS1C - PRL Version	✓	
SS1D - Hardware Version	✓	✓
SS1E - Firmware Version	✓	✓
SS1K - Master Subsidy Lock	✓	
SS1Q - IQAgent Version	✓	✓
SS1R - Carrier	✓	✓
SS1S - Service Provider	✓	✓
SS1T - OEM	✓	
SS1U - MEID	✓	
SS1W - Device Make	✓	
SS25 - Chipset Vendor	✓	
SS28 - Dialer Host Identity	✓	
SS2A - Sourcing Software Version	✓	✓
SS2B - Device Version	✓	
TIOF - Time Off	✓	✓
TION - Time On	✓	✓
UI01 - UI Keypad Event	✓	✓
UI03 - Error Message	✓	
UI08 - Displayed Signal Strength	✓	✓
UI09 - Displayed Battery State	✓	✓
UI10 - UI Booster Pack Version	✓	
UI11 - UI Touch Screen Event	✓	
UI13 - Application Entry	✓	✓

Metric	Embedded	Non-Embedded
UI15 - Application Exit	✓	✓
UI19 - Application Focus Change	✓	✓
UI25 - Application Execution Change	✓	
VC04 - Call Event	✓	
VC05 - Call Manager Event	✓	
VC10 - Booster Pack Version	✓	
VC11 - Call Manager Event Short	✓	
VC12 - Call Manager Event Data Start	✓	
VC13 - Call Manager Event Data Connect	✓	
VC14 - Call Manager Event Data End	✓	
VC15 - Call Manager Event Voice Start	✓	
VC16 - Call Manager Event Voice Connect	✓	
VC17 - Call Manager Event Voice End	✓	
VC18 - Call Manager Event SMS Start	✓	
VC19 - Call Manager Event SMS Connect	✓	
VC1A - Call Manager Event SMS End	✓	