THE CLIPPER GROUP
Navigator™
Navigating Information Technology Horizons℠
Published Since 1993 Report #TCG2007059 May 8, 2007

# HP's DRAGON Does Data Retention Right for European Telecommunications Operators

Analyst: Anne MacFarland

## Management Summary

For many years, telephone companies have been required to supply CDRs (call detail records) to law enforcement officers upon presentation of subpoenas and other forms. Recently, in *Directive 2006/24/EC*, the European Union codified the retention of this data, and the ability to provide it promptly to law enforcement officials. Europe also has a strong heritage of laws protecting the privacy of information about individuals. Information from the records of individual customers cannot be used to support marketing efforts, nor can it be analyzed for Business Intelligence. Only aggregate data can be used.

Compliance with the new Data Retention directive has put Telecommunications operators in a bind. It is not just voice messages that must be kept, but also text messages, SMS, internet Website access, and e-mail. The litany of Websites visited must be part of the record – as must be phone calls where someone let a phone ring three times and then hung up. This is more than just billable calls. There is, as in many places, the complication added by the existence of an additional layer of telecommunications companies that run their calls over networks they do not own. Who owns the data for a particular usage is not always obvious.

HP has a deep heritage in telecommunications, and saw this as an opportunity to design technology to meet very particular, very stringent needs. The data and the entire workflow of providing the information had to be demonstrably secure. HP has been working with demanding European telecommunications companies in Italy and Turkey to perfect a solution that would satisfy the privacy concerns of customers, the time constraints of law enforcement, and the operational and business requirements of the telecommunications operators.

The requirements for capture, retention, retrieval, and secure workflow were draconian. Therefore, it is fitting that, when HP accepted the challenge, it produced an *HP Data Retention and Guardian Online solution* that is abbreviated *DRAGON*[1]. While this solution is designed specifically for the requirements of the telecommunications industry (and, more specifically, for European telecommunications), the exactitude of its solution will be of interest both to telecommunication operators in other geographies and to operations managers in other industries, such as health care, that have their own very exacting requirements. For more details on the specifics of this solution, please read on.

## Requirements Drive Architecture

The requirements to capture all the data flows that passed through the network, not just billable services, meant that the information could not be taken from the billing process, but had to be captured from either the switch itself

IN THIS ISSUE



[1] The words are not related. *Draconian* comes from a punitive code of laws developed in ancient Athens by a man named Draco.

or the mediation platform that underlies the operations platform[2]. For legal reasons, all the information had to be associated with a user (a phone number, or IP address). The solution had to capture all the kinds of data flows that used the operations platforms. Immediately, it had to secure those records against any alteration. It had to keep them at least two years.[3] It needed to provide information to authorized requests in a speedy and totally secure way. These caveats drove three design requirements.

1. **Data management –** The solution had to handle billions, even trillions of various kinds of data records in a sensible way.
2. **Security –** Security had to be baked into the solution at each and every step of the process flow. It had to be provably secure to be satisfactory to law enforcement.[4]
3. **Query retrieval and design –** The solution had to retrieve precisely the right detail records for each request from a very large repository in a way that could support thousands of requests a day.

## The Solution Topology

### *Data Management Layer*

The data management layer is a linear process from the harvesting traffic information from the switch and customer information (CDRs[5]) mediation platforms, into a pre-feeder, loading the Oracle database using HP's high-speed ingestion technology, and then, over time, using an archiver to move older, less-accessed records (usually after 6 months) to a compressed data store. Indexes of the compressed data store allowed records to be accessed from the secondary database with only a 10 to 20% latency (which is not much when you are talking microseconds).

The solution is not particular about what kinds of CDRs it ingests. Down the road with new services that Dragon is asked to address, the problem will not lie in the information being ingested or the storage needed to hold it, said HP's Andrea Fabrizi, the man responsible for developing the DRAGON solution over seven years. Problems would more probably arise about *who produces the information* and where and *how to collect it*, as networks become more layered and multi-functional. The architecture will meet these challenges as they come up, but it is too early to speculate on their nature.

### *Security*

The IT administrators and DRAGON operators must use a secure login, and their actions are captured for each individual in a secure log. The query and retrieval engine captures the query and the owner of the query in an encrypted log. A policy enforcer controls access to data on an individual basis. Optional *Digital Rights Management* extends the security to the fax machines by which many law enforcement officers receive information.

### *Query Retrieval*

For people using the DRAGON, a workflow engine manages requests and their status[6]. The law enforcement officers do not directly access the database. Operators are the only ones to uses the GUI to manage the queries. The operator inserts the data in a report that is faxed back. The digital rights is at work in this layer as well – only the operator assigned to the request can read the fax or send a fax back. Only the relevant law enforcement officer can print out the fax in his office. The actions of individuals involved in a request are all logged, so any leak can quickly be traced to its source.

### *Storage*

Dragon will leverage a full variety of HP tiered storage, including the *StorageWorks XP* and *EVA* storage products, as well as its nearline and offline technologies. In the next release, due by the end of 2007, DRAGON will use *HP RISS* grid storage, whose indexing will remove the need for the Oracle database.

## Go to Market Strategy

HP is using the DRAGON solution to increase its presence in telecommunications accounts. Cisco and Nokia are obvious partners, along with Oracle for the database and AmDocs for its presence in telecommunications billing. HP will go to market side by side with

[2] Conveniently, HP has experience and patented IP in both areas.

[3] While the EU composed the directive, the retention period is set by each country in the EU.

[4] The solution was developed in Italy. In some European countries, members of Intelligence organizations, in certain well-documented circumstances, also have access to CDRs. The access is, of course, limited to a specific request for a specific set of records.

[5] CDRs are Customer Data Records.

[6] It also manages the CDR lifecycle and CDR destruction at the end of the proscribed retention period.

these partners. With a solution like this, the installation is as important as the solution components, if not more so. HP will handle the implementation, which it has optimized. A proof of concept can be set up in one to two weeks, and full installation takes a couple of months.

HP's long history in the telecommunications market (with *OpenCall, OSS*, *BSS*, and *Mediation* software), and its expertise in data retention (with RISS) give it a unique familiarity with market requirements for this solution.[7] HP sees it is the first in a larger set of specifically-architected solutions, focused on industries, like health care, that have demanding requirements for both privacy and use of data. Think of how such a targeted solution might make your operations more secure.

## Conclusion

HP has taken its expertise, applied it to a difficult situation, and come up with a well-targeted solution. Few enterprises, given the option, would want anything less. Consider your draconian problems, and how HP's kind of solution, down the road, might be just what you need.

[7] In the seven years bringing it to market, much IP has been developed and is in the process of being patented.

### About The Clipper Group, Inc.

***The Clipper Group, Inc.,*** is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

- ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

### About the Author

***Anne MacFarland*** **is Director of Data Strategies and Information Solutions for The Clipper Group.** Ms. MacFarland specializes in strategic business solutions offered by enterprise systems, software, and storage vendors, in trends in enterprise systems and networks, and in explaining these trends and the underlying technologies in simple business terms. She joined The Clipper Group after a long career in library systems, business archives, consulting, research, and freelance writing. Ms. MacFarland earned a Bachelor of Arts degree from Cornell University, where she was a College Scholar, and a Masters of Library Science from Southern Connecticut State University.

- ***Reach Anne MacFarland via e-mail at Anne.MacFarland@clipper.com or at 781-235-0085 Ext. 128. (Please dial "128" when you hear the automated attendant.)***

### Regarding Trademarks and Service Marks

**The Clipper Group Navigator**, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group Captain's Log**, **The Clipper Group Voyager**, **Clipper Notes**, and *"clipper.com"* are trademarks of The Clipper Group, Inc., and the clipper ship drawings, *"Navigating Information Technology Horizons"*, and *"teraproductivity"* are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

### Disclosure

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

### Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.