Pipeline
Knowledge Is Power

www.pipelinepub.com Volume 3, Issue 11

Staring Down the Compliance Conundrum

by Joe Hogan and Marc Price

It reads like a spy novel or political thriller. A person of interest is identified. He's accessed jihadist web sites. He's received and made calls from a person who, in turn, has received calls from Afghanistan or Western Pakistan. He has sent a flurry of recent picture messages from a vulnerable national monument. Police move fast to corroborate these facts with other information: a questionable driver's license from a state with lax rules, a recent pilot's license, a money transfer from overseas.

Worldwide communications are essential for our freedom. At the same time they are one of the best means we have to identify early warning signs of impending threats. As in the example above, any single call or event may be insignificant by itself, while in total, these events present a complete profile worthy of interest.

But do operators and governments have all the tools they need to record, track, and correlate such information? The answer is yes, and as the importance of the tools grows, so does the sophistication.

Lawful interception and surveillance mandates have gone from a low-visibility back-office function to a critical need, in an environment where operators may be asked and required to compile millions of customer records in a matter of hours to turn over to authorities. The focus, budget and auditing of the operator's lawful intercept capabilities have thus come to the forefront. Political ramifications aside, this is a very real challenge that service providers have little choice but to face. Furthermore, with the rise to prominence of many different types of data services—text messaging, video and email—this problem becomes even more complex. By way of example, while five voice sessions produce five voice call records, a single IP-based session can produce hundreds, or even thousands of records.

Authorities understand well that a complete picture of voice and data is necessary to greatly improve the odds of identifying a person of interest. Indeed, having such a complete picture narrows the list of possible suspects whereas information from voice calls or data alone would fail to narrow the pool sufficiently.

For operators, the importance of dealing with lawful interception mandates cannot be understated. However, mandates such as the Communications Assistance for Law Enforcement Act (CALEA) in the U.S., and similar mandates in Europe and

elsewhere, have raised a conundrum. How do service providers rectify the tug of war that exists between providing quality and safe service to customers, while at the same time delivering records across a subscriber base of 50 million in a matter of hours?

Furthermore, in addition to CALEA compliance, service providers must also comply with laws such as Sarbanes-Oxley and E911. The problem is that in many cases, a solution designed to satisfy CALEA requirements will not necessarily meet the demands of Sarbanes-Oxley, by providing a comprehensive and visible trail of all accounting functions, or E911, by identifying the location of a caller using a VoIP-based phone service. Service providers are faced with the prospect of shelling out serious cash for individual solutions that satisfy the varying compliance laws.

How did we get here?

Prior to the 1990s the global market for intercept and surveillance products was relatively small and included only the original manufacturers of telecom switching equipment and a few specialized equipment vendors. Surveillance capabilities were comprised of proprietary features leveraging physical wiretapping interfaces available within the switch, as delivered by the telecom equipment manufacturers, or available from specialty manufacturers to support law enforcement agencies. These early solutions were typically installed by the communication service providers on behalf of domestic law enforcement agencies on an as needed basis. Permanent surveillance systems integrated with sophisticated cryptographic analysis were deployed by specialized branches of the military at major international telecommunications interconnect locations (undersea cable and satellite) to support foreign intelligence gathering.

In most of the democratic countries throughout the world these two surveillance capabilities, one designed for domestic law enforcement and the other for gathering foreign intelligence, were historically separated and administered by different courts. In the US, for example, surveillance for domestic law enforcement is overseen by state or federal courts responsible for criminal prosecution whereas surveillance for gathering foreign intelligence, or "counterintelligence," is handled by a special Foreign Intelligence Surveillance Court called FISC.

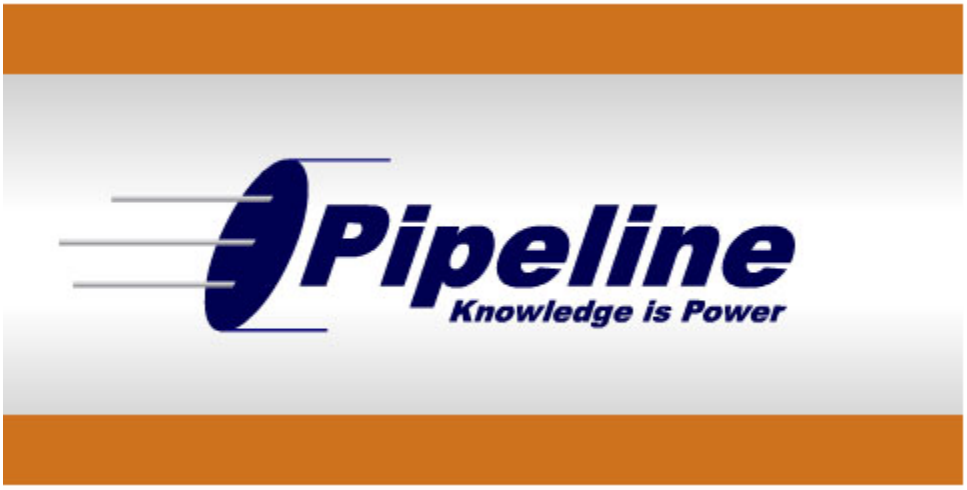
During the initial growth period of the Internet, with e-mail and World Wide Web (WWW) usage rising dramatically, specialized Internet Protocol (IP) surveillance solutions were developed to support evidence gathering for prosecuting early forms of electronic or "cyber" crimes. During the 1990s, child pornography, exploitation, and fraud represented typical cases that occasionally required use of "packet sniffers" for the collection of evidence only available from IP networks.

The passing of (CALEA) in October 1994 and similar laws enacted in Europe catalyzed the market for third party lawful intercept and surveillance solutions. Amendments to existing laws to support packet-mode communications increased the size of the solutions market with the first "converged" LI solutions becoming commercially available by 2002.

Following the terrorist attacks of September 11, 2001, additional legislation was

enacted in many Western countries, and these emerging mandates have largely driven the current evolution of the market.

In general, surveillance mandates across Europe are more rigorous than those currently enacted in the US with a bias towards a standards-based, best practices approach (RFC 2804 – IETF Policy on Wiretapping). The Netherlands came up with a standard for IP interception and championed a framework for electronic surveillance when it held the EU presidency in 2004. Italy leads the world in intercepts per capita, shortly ahead of the Netherlands, and corruption inquiries are perceived as the primary driver for this high degree of activity.



What's on the horizon?

Work continues within CALEA and elsewhere as operators are increasingly being asked to improve their environments to enable rapid responses to government requests for voice and data, even in the face of other regulatory pressures.

In the U.S., the latest figures available from the Department of Justice show that 1.2m requests to tap telephones and email addresses were made in 2005, and while most involved requests for historic telephone call record data, there were 48,000 requests for real-time call data and 2,600 intercepts of communications. These figures exclude additional activity in the U.S. from the controversial warrant-less requests and the work of the National Security Agency.

Data reported by various government agencies requesting lawfully authorized intercepts illustrates an important underlying trend: over 85% of all intercepts executed worldwide are for communications over a mobile or portable device. Thus *roving surveillance* is of utmost importance, and as operator networks for converged service providers grow in complexity with the deployment of next-generation infrastructure, such as IMS, increasing demands will be made on systems that collect and correlate such data.

In the U.S., roving surveillance requirements are specified in Section 206 of the U.S. Patriot Act. This measure has had profound impact on lawful interception methods, since it expands the scope of surveillance beyond a single communications identity to multiple communications identities associated with a target. For example, multiple fixed line and mobile phone numbers, e-mail addresses, SIP addresses, and other identifiers may now be involved in correlating the traffic of various service usage for a particular person or persons of interest.

Finally, in a controversial ruling, the Federal Communications Commission (FCC) has required that operators of broadband Internet and interconnected Voice-over Internet Protocol (VoIP) services establish systems to enable law enforcement agencies to process wiretapping requests. While standards are not finalized for this technology, it is clear that these services are next to be brought under surveillance and control.

Other legislative concerns

In the meantime, the Wireless Communications and Public Safety Act of 1999 required as a feature of the 911 emergency-calling system that operators automatically associate a physical address with each calling party's telephone number. This data enrichment was unneeded for broadband and VoIP services until recently, when in 2005 the FCC required that VoIP services that interconnect with the public telephone network begin to provide 911 service, as well as provide notice to their consumers concerning the 911 limitations. As mandated, the E911 hookup may be directly with the wireline E911 Network, indirectly through a third party such as a competitive local exchange carrier (CLEC), or by any other technical means, although some VoIP providers remain significantly out of compliance with the order.

The Sarbanes-Oxley Act was established in 2002, requiring that all operators' internal systems and operational controls, pertaining to business activities and financial reporting, produce audit evidence that can be tracked, monitored, and ensured by the management team of the companies.

In short, above and beyond the operators' own requirements to collect, mediate, store, and distribute call records for service usage, there is increasing pressure to handle processing of this service usage for other reasons, often in real-time, and sometimes involving very processing-intensive correlation and business rules.

How is all of this done?

The lawful interception standards proposed by ETSI have provided the dominant reference model that is currently applied in Western countries worldwide. Although there are slight variations in terminology according to region and to address specific verticals (e.g., Cable/MSO), the ETSI model is essentially the same as the predominant architecture deployed throughout the U.S. to achieve CALEA compliance.

See *Figure 1 – Lawful Intercept Reference Model* representing a composite view based on ETSI and TIA standards and terminology.

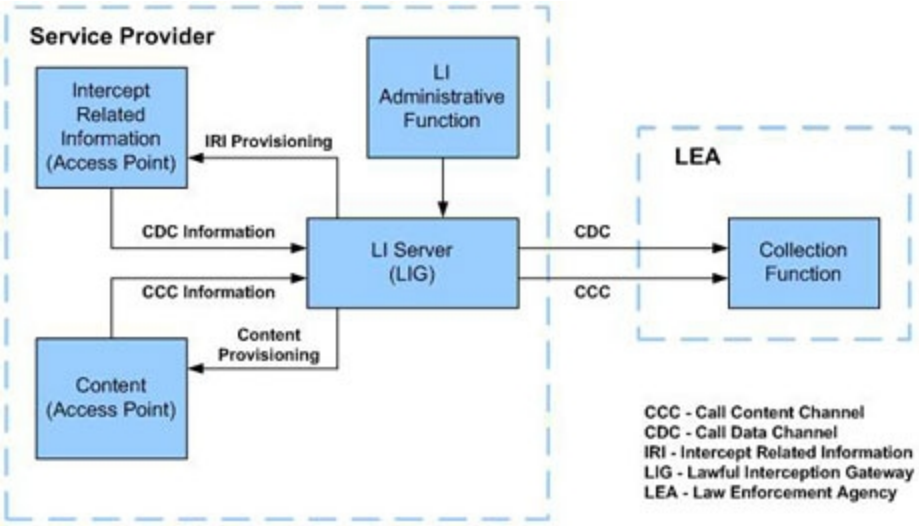


Figure 1 – Lawful Intercept Reference Model

The Lawful Intercept Server is responsible for direct interaction with the Access Points for both Intercept Related Information and Content. This, in fact, should be as best as possible a view of the raw data as provided by the switch, soft-switch, or gateway hardware producing records of the service usage involved.

The Lawful Intercept solution must have an Administrative Function, whereby an operator shall administer the rules pertaining to the network equipment involved and the correlation and business rules for the services deployed. Finally, the Law Enforcement Agencies must have direct access to the system via a Collection Function, with real-time and batch reporting capabilities to adequately address the needs described above.

Operators deploying such solutions note that this is one of many such systems in the environment responsible for network collection, data enhancement, correlation and analysis, and data retention. With other challenges at hand, such as Sarbanes-Oxley, and E911, should operators deploy different solutions for each of these initiatives, or should they try to fulfill each of these requirements with a single system?

The answer is dependent upon each operator's unique environment. However, there are certain guidelines that may be applied in all cases:

Pure Sources of Data

More than any single factor, the need for pure sources of data dictates that lawful interception and surveillance must be done at the network edge. Data that is enhanced or altered is of less value to law enforcement agencies than data straight from the access network, and in fact many agencies are now mandating that

operators deploy solutions to meet this requirement.

In fact, this type of solution is of great benefit to any operator, because a solution capable of collecting from the original raw sources of data can operate upon that data in many ways. For example, while the raw data may be used to execute correlation and business rules for legal authorities, the same data can be enriched and enhanced in a separate parallel thread in order to provide E911 data, as well as accounting data for the operator's internal systems. Finally, such systems must produce a clear recorded trail of all activities as well, particularly if any business or financial data is involved that may enter the accounting stream.

Data Storage and Retention

Data that is captured is only useful for as long as it is stored. While some information is provided and used in real-time, the majority of transactions remain historical in nature, meaning data storage is required. An important use of subscriber call records is to identify social network (calling) patterns that may indicate an imminent terrorist threat by subjects of interest. This type of application is not possible without a large database of historical usage. However, not all of the service data need be stored in its raw form. As long as the lawful intercept and surveillance system has access to the raw data, it may then strip down and store only the data for the elements needed in future correlation. For example, it is not essential to retain all of the data packets involved in every picture message, although it might be quite interesting for officials to know that several picture messages are being taken by persons of interest, from the cell in or adjacent to the Sears Tower.

Correlation and Business Rules

The most common activities pertaining to lawful interception, surveillance, and traffic analysis involve the function of mapping common addresses such as phone numbers and e-mail addresses to applicable network identifiers. The emergence of SIP addressing and IP based signaling for VoIP has accelerated the need for more flexible methods for performing extremely fast database lookups in support of real-time enrichment of raw network usage data.

Cross correlation of session and call data information for multiple service types (e.g., voice, email, SMS, MMS, IM, etc.) is greatly increasing the value of actionable intelligence for prevention or apprehension. It is for this reason that solutions supporting both voice and data are in such demand. Of course, as shown above, other initiatives like Sarbanes-Oxley and E911 have also crossed domains, and now involve the attention of wireline, wireless, broadband, and cable providers.

Concluding thoughts

Service providers face greater challenges than ever before to meet the myriad of complex mandates, with increasingly severe consequences of failing to comply. Ultimately, implementing a lawful intercept and surveillance solution and strategy is no longer a choice; it's a necessity to survive in today's hotly-competitive market. Forward thinking operators will seek to put solutions in place that solve these

problems, in conjunction with other issues and challenges, such as compliance initiatives for E911 and Sarbanes-Oxley. The world's ability to identify interrelationships amongst the enormous volume of data for communication services grows daily. Operators should view this as an opportunity to implement solutions with internal benefits as well.

If you have news you'd like to share with Pipeline, contact us at editor@pipelinepub.com.