SUBSENTIO

TOGETHER WE'RE SAVING LIVES™

September 2020

NEWSLETTER

Your Trusted Third-Party Compliance Company

Welcome to the Subsentio Quarterly Newsletter

In This Issue:

Changing the Narrative on Legal Demand Services

A New Public Safety Eco-System

Steve Bock, CEO & President

The legal compliance industry historically has worked in highly inefficient silos. To compound this inefficiency, the laws have not kept up with technology and the technology used by the people needing to be investigated (spies and criminals) always seems to be a step ahead of those in the law enforcement community that are trying to keep pace. We intend to change that.

Today, our work at Subsentio falls into two primary services, subpoena compliance and lawful intercept. Both of these services consistent of multiple functions stemming from a lawful request. The first is acquiring raw subscriber data out of the communication service provider network, then mediating or formatting the data to send it to law enforcement or the requesting party. This often results in providing law enforcement massive amounts of disparate data to analyze. Subsentio has focused on lawful intercept services to provide cost effective electronic surveillance that was delivered quickly to law enforcement. When a life is at stake, law enforcement needs data and intelligence immediately.

Over the years, however, lawful intercepts are not the biggest pain point for investigators, it is subpoena compliance by a long shot. Why? Many of the challenges that exist in lawful intercept are magnified when it comes to acquiring and

SUBSENTIO

TOGETHER WE'RE SAVING LIVES™

September 2020

In This Issue:

deciphering call records. To begin with, the sheer volume of requests is staggering with well over 1 million subpoenas issued in the United States annually. Since there is no cost recovery mechanism many carriers spend as little as possible to comply, which sometimes results in law enforcement waiting months for their data and intelligence to further their investigations.

Further, unlike lawful intercepts there is no standard formatting or rules for the data that's delivered. We've seen call records delivered in screen shots, all types of csv files and faxes of unintelligible data. Law enforcement analysts have had to resort to using colored markers to high light telephone numbers on stacks of papers to connect the dots in an investigation. It's no wonder that law enforcement can spend days and even weeks trying to sift through and decipher what should be easy to understand, actionable intelligence.

What is needed is a Public Safety Ecosystem. If these functions were integrated, many investigators could save lives and solve crimes almost with the push of a button. The need has never been greater so we at Subsentio intend to provide those services We're going to create standards for the way call data is delivered by formatting call records into consistent, useful files, add intelligence through enhanced forensic tools and provide it in days, not weeks or months.

Every week Subsentio helps law enforcement save more lives through the legal demands of a subpoena compliance, but we can do better, faster, and with great efficiency. We're going to change the narrative that it's not okay to continue providing poor service because "that's the way the industry has always done it." By integrating the functions seamlessly, Subsentio is going to set the standard for a new Public Safety Ecosystem that will save time, money and most importantly, it will save lives.

SUBSENTIO
TOGETHER WE'RE SAVING LIVES™

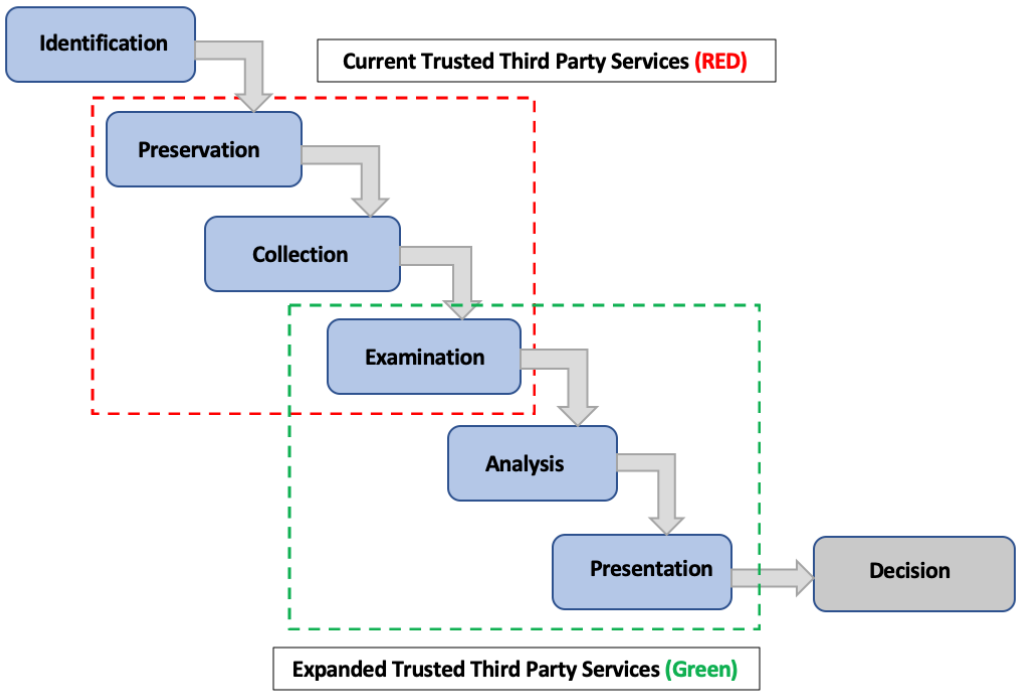
September 2020

Subsentio's Trusted Third Party Participation in the Investigative Process

Tom Gudsnuk, Esq., General Manager

Providing lawful intercept and subpoena compliance services is an intricate web of laws, policies, regulations, rules, and processes that require extensive training with strict adherence and understanding of the full impact of the specific functions for the overall success to fulfill, complete, and protect the integrity of the investigative process. As a Trusted Third Party (TTP), Subsentio participates in providing vital functions supporting the collection and delivery of the requested and mandated information.

The investigative process is governed by specific rules from the laws passed by the legislature, regulations, court rules, and law enforcement rules and procedures. These may vary by jurisdiction by country, region, state, or local aspects. Investigators are highly trained in following the prescribed methods. A diagram of the general process is depicted below, with and overlay of Subsentio's services participation.



Investigative Process Digital Framework

In a typical investigation, the investigating authority identifies the need to perform the investigation. This can be from law enforcement or a civil authority with the requisite ability to undertake such an investigation. Upon meeting their criteria for pursuit of information, the result is a formal request for the digital information. In the Communication Service Provider (CSP) area the formal request is manifested by issuance of a subpoena, warrant for the information, an administrative subpoena, lawful intercept request, national security letter, Grand Jury Subpoena, or a Court Order to the CSP for the information. The type of request is dependent upon the type of investigative process being conducted.

When a request is received, the CSP must act on that Court Order and produce the requested materials. As a Trusted Third Party, Subsentio provides the services to recommend, integrate, and manage the process for the CSP. First the request must be validated by the professional staff that is trained in performance of the review criteria, and often must coordinate with the requesting party to adjust the conformity of the request to meet the appropriate criteria and authenticate the delivery manner. Sometimes, due to the nature of the request, there is a highly secured delivery methodology used to protect the integrity of both the information and the confidential nature of the investigation. Once validated, the information is preserved, collected, and verified for submittal as the answer to the request. At each step in this portion of the investigative process, the steps, handling, and methods are specifically documented and tracked to create an audit trail that validates the integrity of the process for possible evidentiary usage of the produced information. Incumbent in performing these tasks is the ability and capacity to produce, collect, and handle the information, which in sophisticated communication networks involves tying into technology solutions implemented for those very purposes. These services are identified in the red box in the framework diagram.

The investigative process doesn't merely end once the information is produced and delivered. The investigators getting the information now must make use of the data to further or complete their investigation. The examination, analysis, and presentation of the information is key to the investigator's efforts and is often very time consuming. Correlating the data is difficult and the ultimate task is for the investigator to convert the data to actionable intelligence. Fortunately, there are a myriad of technology tools available to assist in those efforts, however the tools are often expensive and not available for all investigations. The services identified in the green box in the framework diagram are those services where Subsentio is expanding the service offerings that will include more cost-effective ways for turning the data in to actionable intelligence for investigators at the national, state, regional, and local levels. This greater efficiency will not only reduce costs, it will expedite assistance to the investigator, and carry forward Subsentio's motto – Together We're Saving Lives ™.

Security – Taking Into Account The BIG Picture

Todd McDermott, Chief Security and Operating Officer

As we all know security breaches of data repositories which include personal and private information is headline news. The best examples of those incidents are those that hit the media and affect millions and millions of consumers. Good examples from the retail sector are Target and Home Depot which collectively lost over 160 million records. One of the most publicized data breaches involved the US Government Office of Personnel Management which lost upwards of 21 million records in 2015. Not to be outdone but the US Postal Service had a breach which affected upwards of 60 million records. Suffice to say people became concerned and IT security became paramount. But we forget about the BIG picture.

In law enforcement investigative support activities, a significant amount of "sensitive" and sometimes, Classified information is shared with companies and is transported through a companies' facilities. There is significant focus on secure transport through VPNs for the real-time delivery of communications traffic but what about the "data at rest"?

Service providers and trusted third parties are trusted with unique identifiable information associated to active investigations. Key information such as telephone number, target name, address etc. may be presented to the staff to support legal process and to provide them the necessary information to fulfill the mission; records production and/or lawful intercept. What this means is people outside of law enforcement are privy to information if, unknowingly or intentionally publicized, will compromise an investigation and breach the trust. The BIG picture includes personnel.

A very simple principal is applicable here: If you share a secret with one other person it is no longer a secret. The fundamental concept of "need to know" minimizes the risk. Staff that have a responsibility to do the work must understand the sensitivity of the information they can become privy to. Restricting access to this information and not disseminating it even with co-workers must be routinely reinforced to the staff along with the principal of "need to know".

People may be a company's strength but may also be a weakness. Trust is earned by continued demonstration of adherence to one's security policies and guidelines. Not only IT security but personnel security, is critical. Companies must realize that sensitive and/or Classified information is first presented to their staff. Security begins here and is a part of the overall "BIG Picture" security which must be addressed.

At Subsentio our staff understand and respect the fact that we are charged with keeping very sensitive information on behalf of our customers and law enforcement. The “need to know” philosophy is retained with respect to all our operations and regularly emphasized with all the staff. Also, without question, our IT security for our systems, infrastructure, our data at rest and that being transported is always considered critical and must be maintained at the highest levels possible. Subsentio is truly committed to address the BIG picture.

Cloud Security Awareness and Evaluation

Shawn Hannon, Chief Information Security Officer

Subsentio is a leader in the Trusted Third-Party (TTP) Lawful Intercept and Subpoena processing Industry and Information Security (InfoSec) and innovation are cornerstones supporting this leadership position.

Without a resilient, comprehensive, and proactive approach within our InfoSec’s core objectives our innovation and leadership status would diminish or not exist.
Information security involves protecting the confidentiality and integrity of data and the ensure data availability. At Subsentio, the InfoSec team normal operations take the following types of measures to meet data security:

- Organizational/Administrative controls specifying who can perform data related operations such as creation, access, disclosure, transport, and destruction.
- Physical Controls relating to protecting storage media and facilities housing storage devices.
- Technical Controls for identity and access management (IAM), encryption of data, at rest and in transit, and other audit-handling requirements for complying with regulatory or legal requirements.

When Subsentio decided to offer lawful intercept and subpoena processing services and products in a cloud ecosystem the InfoSec team considered and evaluated the possible impacts it would have on information security. There are numerous considerations, for example, the quality of the cloud’s infrastructure implementation, the attack surface of the cloud, the likely pool of attackers, system complexity, and the expertise level of the cloud administrators and support teams. Unfortunately, in the early days of the cloud ecosystem, at first none of these considerations seemed decisive regarding cloud security and there were no obvious answers when comparing cloud to non-cloud systems as to which is likely to be more secure in practice.

However, further into the examination process the InfoSec team started to recognize that numerous cloud providers handled cloud and information security risks as a shared responsibility. In this model, the cloud service provider covers security of the cloud itself, and the customer covers the security of what they put in it. Most cloud computing security risks are related to cloud data security. Whether a lack of visibility to data, inability to control data, or theft of data in the cloud, most issues come back to the data customers put in the cloud. Protecting cloud data requires visibility and control. The InfoSec team understood that this protection would need to be broken down into the following phases:

- Understanding cloud usage and risk
  - Identify sensitive or regulated data
  - Understand how sensitive data is being accessed and shared
  - Discovering unknown cloud use
  - Audit configurations
  - Uncover malicious user behavior
- Protect your cloud
  - Apply data protection policies
  - Encrypt sensitive data with your own keys
  - Limitations on how data is shared
  - Stop data from moving to unmanaged devices you do not know about
  - Apply advanced malware protection
- Respond to cloud security issues
  - Require additional verification for high-risk access scenarios
  - Adjust cloud access policies as new services come up
  - Remove malware and threats from a cloud service

Again, there is security of the cloud – which is the responsibility of the cloud provider and protects the infrastructure that runs all the services offering composed of hardware, software, networking, and facilities. Then there is security in the cloud – which is the responsibility of the customer and determined by the services and products the customer selects and/or deploys.

Below are examples of some of the controls that can be used when evaluating cloud and information security protection.

- Inherited controls: Physical and environmental controls - the customer fully inherits then from the cloud provider
- Shared controls: Patch management, configuration management, awareness, and training - which apply both to the cloud provider and customer
- Customer Specific: services and products based on the applications that the customer has deployed in the cloud ecosystem.

With the implementation of this evaluation process the Subsentio InfoSec team has confidence to operate our Trusted Third-Party Lawful Intercept and Subpoena processing services and products securely and successfully in a cloud ecosystem. They meet our core security and compliance requirements, such as data locality, protection, and confidentiality with a set of comprehensive security services and features allowing us to shift some of our focus to scaling and innovating our core business.

Communication Service Provider Mergers and Acquisitions: Legal Compliance with Lawful Surveillance Laws

Bill Ekes, Chief Revenue Officer

As you are likely aware, being competitive in the Communications Service Providers (CSPs) industry you must form partnerships. These often lead to mergers and acquisitions forming larger and more competitive networks. All these companies are required to be compliant with all government mandates. The compliance aspects are typically viewed through the lense of having federal approval in multiple jurisdictions along with the Federal Communications Commission (FCC) and or state regulatory PUCs/PSCs requirements. Tariffs and licenses filings often overshadow historical record subpoena and lawful intercept compliances. In many of the mergers or acquisitions the due diligence process may not address lawful surveillance equipment, processes or even perhaps even compliancy.

Sometimes an afterthought on a CSP's agenda may be where they stand with providing the government's compliance for lawful intercept and historical data subpoena support. They rightfully concentrate on their core business of combining networks and personnel for streamlining operations and revenue. This results in the merged CSPs working out process changes, network changes, back office (billing) changes, making sure all filings are done and most importantly, they are providing quality and enhanced service to their customer base. A key process that needs to be addressed in these instances are the legal responsibilities for being compliant with LI laws and how it will be done moving forward.

Subsentio can immediately help by offloading these duties and responsibilities for compliance with the laws. Here are some of the ways Subsentio helps:

- Subsentio's Trusted Third-Party (TTP) services takes all the burden away from the CSP and reduces the financial costs by providing an economical manner from legal review, lawful compliance management and interfacing with law enforcement
- Subsentio manages existing platforms if one of the CSPs made the investment in purchasing LI equipment
- Subsentio provides consultative services and recommends the best approach for the future including procedural processes

Subsentio has been providing lawful surveillance support to more than 300 companies globally for more that 16 years. This is our business. Let us help you keep your focus on your core business.

Trusted Third-Party Benefits for Communications Service Providers

Mark Bolton, Director of Product Development

Legal demand response expertise

Responding to legal process while protecting customer privacy rights, is important and necessary, but typically not a core competency for Communications Service Providers (CSPs).

For many small and medium CSP's the prospect of securing inhouse expertise to properly handle the wide variety of legal demands will be difficult to justify. A Trusted Third-Party (TTP) provides cost effective access to the kind of expertise needed to respond to legal demands quickly, accurately and efficiently.

Cost effective and fully compliant

TTP's can provide both the technical solutions and the related compliance program needed to be fully compliant. By spreading the cost for these programs across many CSP customers TTP's make compliance much more cost effective. TTP's are exposed to a greater volume of legal request and a wider variety of the type of requests. This experience will insure a proper balanced response thereby protecting the reputation of the CSP with their customers and law enforcement. This balanced approach of protecting customers privacy and responding to Law enforcement with timely and accurate information is vital.

Technical solutions

TTP technical solutions offer an improved total cost of ownership over a standalone solution from a capital expenditure and operating expenditure perspective. Most technical solutions for lawful intercept compliance include network specific components and centralized management and provisioning systems. TTP's can leverage high volume purchasing power for these systems and share the common management systems among several customers to offer a more cost- effective solution. Additionally, the engineering expertise to maintain them is shared and the level of experience is much greater than the typical "collateral duty" for most in house engineering teams.

5G Impact on Lawful Intercept Considerations

Marcus Thomas, Chief Technology Officer

5G is transforming industries like healthcare, manufacturing, transportation, and others. The Internet of Things (IoT) is on the rise. The number of connected devices is set to increase almost four-fold to 3.2 billion by 2023. While there are several factors contributing to this rise, one of the most important is the development and implementation of 5G networks. Why is 5G leading the transformation? 5G is lightning fast and has greater reliability than current and historical mobile networks. Further, 5G networks can support an almost unlimited number of end devices, and has ultra-low latency, making it a perfect platform for those low-latency applications like smart cars, health sensors, and traffic management.

What is the impact of 5G on lawful interception? Besides the challenges associated with capturing data in super high bandwidth with massively distributed networks and monitoring extreme volumes of data, 5G networks will also carry a much higher proportion of encrypted data. For law enforcement, these challenges begin with the recording, storing and managing this massive amount of data, only to be faced with the fact that most of it will be undecipherable to them. On top of this, it is certain that a shrinking proportion of that data, even if they can decipher it, will be of limited evidentiary or intelligence value to them. This situation raises serious questions including the fourth amendment requirement for particularity with which an item to be seized is to be described and the scope of the search for it.

When wiretap laws were first passed, in 1968, people used the telephone network to communicate with others. Criminals were no different and used the telephone to plan and execute their illegal activities and communicating with their co-

conspirators. Although networks and telephone devices have changed significantly in the past 50+ years, the way people use telephones (or at least telephone apps) has not changed that much. With 5G networks, criminals will still use mobile devices to communicate their criminal escapades. However, unlike the networks of the past 50 years, the communications of criminals on 5G networks will constitute a very small amount of the traffic flowing over those networks. Law enforcement officers, if they follow decades-old strategies, will be required to wade through massive amounts of information that they know may be useless in order to find the few nuggets that they intend to seize. The process begins to look more and more like a general search. Historically, telephone wiretaps were monitored by live monitors and seizures were made on a per-call and even per-conversation basis. With modern nigh-speed networks, law enforcement has been required to do more post-acquisition minimization.

One possible solution is to make the search and seizure of intercepted information more surgical. However, implementing interceptions in networks with surgical precision without the large proportion of data that is not of interest to law enforcement may require more complex systems. For example, interception systems of the future may require the ability to allow law enforcement to request information on demand by passing instructions into the network from their collection and monitoring systems. Such capabilities have profound implications for security and cost, but, in the end, this type of capability may be necessary to contain the growing burden on both network providers and law enforcement.

* * * * * *