SUBSENTIO

TOGETHER WE'RE SAVING LIVES™

June 2020

NEWSLETTER

Your Trusted Third-Party Compliance Company

Welcome to the Subsentio Quarterly Newsletter

In This Issue:

What's Next?

What Does Subsentio's Leveraged Buyout Mean For The Industry?

Steve Bock, CEO & President

On May 5, 2020 we announced a Leveraged Buy Out (LBO) of the investors in Subsentio. Under the terms of the transaction, ownership will revert to me. What is the impact of the LBO on the industry that we serve?

I did not start Subsentio to get rich, I started it to help US Law Enforcement in the mission of keeping America safe. Over the years, the mission expanded to helping Law Enforcement around the world. That mission cannot be achieved in a silo; it is a partnership that requires cooperation between our communications service provider customers and our vendors to deliver actionable intelligence to law enforcement as quickly as possible. It is a noble cause but far too often we as an industry fail to meet the mission.

In the 20 years that I have been working in the telecommunication legal compliance industry, there has been little to no innovation. The laws do not keep up with the technology and the technology used by the spies and the crooks always seems to be a step ahead of those in the white hats that are

In This Issue:

trying to keep pace. We intend to change that.

That cannot be done if we follow the typical business model of building a business for the sole purpose of cashing in quickly. As a founder that is a temptation, but my view of success has changed over the years. The way I measure success today is not how much money is in the bank account, or how much profit we have made. Instead, I measure it by how many subscribers rely on Subsentio to keep them safe. Today it is in the tens of millions, I intend to make it hundreds of millions.

It will not be easy, and it will not happen overnight, but the Leverage Buyout allows me to change our strategy from short term gains to long term planning. The LBO is a statement that Subsentio is here to stay; we are not going anywhere. Instead, we are going to leverage some of the best and the brightest talent in the industry to create a company that is trusted for public safety around the world. As our new tag line states, we are in the public safety business because TOGETHER WE'RE SAVING LIVES™.

5G and Its Impact on Lawful Interception (LI)?

Marcus Thomas, CTO

What is the impact of 5G on Lawful Interception (LI)? More than 25 years ago, CALEA stood for the proposition that developing networks and services with LI in mind was a critically important behavior, and government and industry made significant strides in developing LI features into (then) emerging networks. Unfortunately, it has also been the general practice for some manufacturers of telecommunications

equipment, and operators of telecommunications systems, to allow the capabilities for LI to lag, and many systems have been deployed without these critical capabilities operational. Now, with the advent of 5G, the need for LI capabilities to be a fundamental part of the service and network design from the outset is lessened, and this may represent a significant benefit to the manufacturers, and operators of communications systems as well as law enforcement agencies.

The heart of the 5G network will be the 5G core. But the network will also depend heavily on the massive speeds made possible by a 5G radio network. The 5G core architecture is defined as a cloud-aligned services-oriented architecture that supports service delivery via wireless, fixed or converged networks. The essence of this description is that 5G allows service providers to bring services to users, rather than using the traditional method of getting users to the service.

What impact will the rollout and overall mainstream adoption of 5G have on communications services? Initially, it simply enables connected devices to communicate in speeds that are orders of magnitude faster than now. Users will still connect to services operated in central cloud networks. As 5G grows, the network will be transformed to bring the cloud to the mobile edge of the network—near the users—billions of them!

Verizon has said that it "is developing its 5G network to serve the most complex use cases imaginable—and those that have yet to be imagined" (Emphasis added.). While bringing complex computing to the "edge" of the network will help solve problems of latency, bandwidth and security, it can introduce substantial challenges to the traditional approach of performing LI at the network's core. As the support for substantial compute-intensive and bandwidth-intensive services begin to appear at the edge of the network, it is essential that LI functions also exist at those edges. Like the services they target, LI functionality must be mobile, orchestrated, and ephemeral.

What are the challenges involved in bringing LI functions to the 5G edge? Essentially, they track many of the problems that are solved by bringing services to the edge in the first place—namely latency, bandwidth, and security. Additionally, awareness of user presence, scalability, short time-to-market, and many other issues present real challenges. CALEA was established to support law enforcement, but the Act's intent was to "…make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes…" while protecting the individual's right to privacy. Conducting 5G intercepts on the edge will present new

challenges related to protecting the privacy rights of most subscribers who are never targets of LI.

Compliance with LI mandates is a complex process whose success hinges on advanced technology, in-depth knowledge of the LI processes, and close attention to privacy protection.

Fortunately, the power of the architecture of 5G is that it represents a platform for resolving these complex issues. Soon LI solutions for 5G will, like the services they intercept, utilize the fundamental flexibility of the 5G network environment to solve many of the same problems the services exist to address.

Lawful Interception Challenges and The Cloud Act

Todd McDermott, COO

The trend to push more and more telecommunications services to be cloud based and using over-the-top communications apps as well as wi-fi based telecoms has introduced lawful intercept challenges to Law Enforcement. Technically, intercept solutions may still be able to be engineered however the real “anchor” of the solution is the Intercept Access Point (IAP). Traditionally the IAP was anchored on the switch or network element serving the targeted subscriber. Simply speaking, the IAP was physically located in the same country as the target and the investigating LEA.

Now introduce virtualization to the communications infrastructure. Subscribers use other means to establish their communications such as routing through the Internet to the carrier’s core and this data stream is encrypted. To gain access to the unencrypted communications, the IAP may now be limited to the core elements which serve the carrier’s entire customer base – globally. Place these network core elements in a foreign country the LEA has serious challenges obtaining authority to enable the intercept.

Historically cross-border assistance between law enforcement agencies has been facilitated through the MLAT process. For those who have experienced trying to secure an MLAT to support an investigation you will know about the significant challenges, delays and “red tape”. When given the option to seek an MLAT many investigators have chosen to drop the issue and use other investigative techniques knowing the potential significant value of the intercept evidence is lost.

An innovative concept has been proposed by the US Government to try to address these technical/jurisdictional obstacles; the "Clarifying Lawful Overseas Use of Data Act". Very apropos; the CLOUD Act. The intent being to give authorities a means to have a more permanent legal arrangement allowing each country party to the agreement the means to affect a lawfully authorized electronic surveillance in the other jurisdiction. There are obvious conditions associated to the implementation of intercepts under the CLOUD Act, but it truly streamlines the capability without seeking a specific MLAT for an investigation.

The US Attorney General is quoted; *"The CLOUD Act was created to permit our close foreign partners who have robust protections for privacy and civil liberties, such as Australia, to enter into executive agreements with the United States,".* Australia has entered formal negotiations to establish the bilateral agreement and become a signatory to the CLOUD Act. The UK was the first country to establish an agreement under the CLOUD Act and there have been discussions about the same in Canada.

Virtualization of telecom networks and the associated communications is becoming more prevalent and the need for the continued capability for lawful intercept remains vital, both technical and legal challenges should be addressed and overcome. There seems to be policies and laws as well as technology in the making to do so; until the next hurdle is presented to our industry.

As a global Trusted Third Party, Subsentio tracks these trends very closely and ensures our customer base is aware of regulatory and/or legislative changes that may affect their obligations associated to lawful authorized electronic surveillance and legal demand processing.

A Lawful Interception (LI) Homecoming

Why I came Back to LI and why Subsentio?

Tom Gudsnuk, General Manager

Let me first introduce myself. I am Tom Gudsnuk, the newly appointed General Manager of Subsentio, LLC. Subsentio is the industry leader in Trusted Third-Party CALEA compliance. If anyone had told me year ago that I would be back in a LI company I probably would have dismissed the comment. However, a convergence of events has made the decision to return to LI relatively easy.

The first compelling event was assisting my former colleague and friend, Steve Bock, in regaining complete ownership and control of the dynamic company he founded many years ago. Upon the conclusion of that effort the rest fell into place since many friends and former colleagues, for whom I have great respect, had already joined up with Steve to continue to help communication providers be compliant with the LI requirements.

Subsentio is a unique company that supports the law enforcement and intelligence communities in the service they perform by handling the heavy lifting of compliance for communication providers. Joining Subsentio is basically a homecoming for me.

The Importance of CALEA

CALEA is the acronym for The Communications Assistance for Law Enforcement Act, also often referred to as the "Digital Telephony Act". It is a United States Federal wiretapping law passed in 1994, during the presidency of Bill Clinton. CALEA's purpose is to enhance the ability of law enforcement agencies to conduct lawful interception of communication by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have built-in capabilities for targeted surveillance, allowing federal agencies to selectively wiretap any telephone traffic; it has since been extended to cover broadband Internet and VoIP traffic.

The importance of CALEA is obvious and it is an important tool for use by law enforcement and the intelligence communities.

My first exposure to CALEA was twenty years ago when I transitioned from the practice of law and joined a telecommunication equipment technology company. That company was a leading manufacturer of CALEA products for the communication providers. Aside from being drawn to the product segment and being involved in all aspects of the technology deployments, I had personal reasons to be interested since CALEA's purpose had a relationship to many of my friends and relatives who were at various levels of law enforcement, detectives, prosecutors, attorneys, and judges. I immersed myself into CALEA and read through the legislative history and the annual reports to Congress.

The thing I noticed most at the CALEA technology company was the industry's limited approach to CALEA and a view that it was strictly a technology solution. Granted, a significant part of a successful CALEA deployment is related to the technology and at

times a complicated network integration. That limited approach, however, doesn't take into account a myriad of other issues related to CALEA and the original purpose of the law. There is a regulatory aspect for compliance by communication providers. There is a reliance by law enforcement for the production generated by the CALEA to save lives or otherwise perfect evidence for later proof in a Court proceeding. There is a cost aspect for the communication providers. You don't have to go too far to see in the footnotes to the annual reports to Congress that CALEA has helped make the U.S. a safer place with instances of removing drugs from the streets, convicting criminals, thwarting death threats, stopping human trafficking, and stopping other nefarious activities or potential threats to national security.

Why Subsentio?

As mentioned earlier, I was once a practicing attorney, involved in all the pieces of either prosecuting or defending a case in the Courts. This included everything from issuing subpoenas, submitting and answering discovery requests, and reviewing warrants to effectively present or refute evidence according to the established precepts. Thus, CALEA is not just about technology. It must include all the related aspects that the law was originally passed to address.

Subsentio is a unique company. Their approach to CALEA is holistic. The company culture centers around a complete comprehension of all the parts of CALEA being intimately interconnected: technology; the law enforcement needs; regulatory compliance; and the intricacy of the communication provider network elements and cost. There is no company that rivals the experience of Subsentio.

The team members at Subsentio are industry experts in all aspects of CALEA. They include communication provider network experts, former law enforcement officers, analysts, and regulatory experts. Many of the staff were the people that helped shape the CALEA laws and standards. It is humbling to be joining the ranks of such stellar market movers in CALEA.

So back to the question: Why Subsentio? The answer is simple, it is like coming home and picking up the charge to help support the fine mission of making the world a better place with such a fine group of people. The decision was quite easy to make – Subsentio makes a difference.

June 2020

Subsentio's Proactive Approach to Corporate Email Security and Protection

Shawn Hannon, CISO

In this age of rising social media and ubiquity of ecommerce spammers and phishers have a tremendous financial incentive to compromise and exploit corporate email traffic. These exploits could enable bad actors' access to user account passwords, bank accounts, credit cards, or even impersonating a corporate office. Simply intercepting and inserting credible signatures or company logos could give a comprised email message instant legitimacy. Protecting the companies trusted well-known brand name is a critical element of any Cybersecurity program and making email traffic authentication, email message monitoring, and the ability to debug email vulnerabilities is a high priority at Subsentio.

Subsentio's Information Security team recognized this early on and explored viable options and approaches to solve this obligation. Identifying the right security solution for a given ecosystem consist of five key elements - Identify, Protect, Detect, Respond, and Recover.

- **Identify** – physical and software assets, business environment, cybersecurity policies, asset vulnerabilities, risk management, supply chain management.
- **Protect** – identity management, empowering staff through awareness and training, data security, information systems and assets.
- **Detect and Respond** – security anomalies and events, continuous monitoring, procedures to effectively response to cybersecurity events and react using incident response plan.
- **Recover** – implement and follow a consistent and current business continuity and disaster recovery plan.

The information security team investigation determined that Domain-based Message Authentication Reporting and Conformance (DMARC) would address our security concerns regarding email exploits along with improve our email messaging authentication, 24/7 monitoring, and vulnerability isolation and quarantine.

A brief overview of how a DMARC policy works – it allows an email sender to indicate that their email messages are protected by two other authentication techniques: domain keys identified message (DKIM) and sender policy framework (SPF). DKIM is an email authentication method that validate an email domain address by using a digital signature. SPF is a path-based authentication method designed to detect forging sender addresses by validating and authorizing the sending mail envelope-from addresses in the domain using the DNS records.

DMARC combines these two authentication techniques to authenticate, control, and monitor corporate email traffic and because our IT infrastructure is hosted at Microsoft 365 implementing DMARC on our Microsoft Exchange was straight forward and quick to execute.

The Replacement of Team Telecom for Foreign-Owned Communication Service Provider Review

Joel Margolis, Esq., General Counsel and EVP Government Affairs

On April 4th President Trump issued an order titled "Executive Order Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Sector" (the "EO"). The EO will replace Team Telecom with a more senior, formal governmental authority to review applications for foreign investment in the US telecommunications sector.

What are the implications of the EO for foreign-owned communication service providers (CSPs) that want to enter the US market?

Background on the EO

Until now, Team Telecom was the inter-agency body that reviewed potential threats to national security and law enforcement posed by foreign-owned CSPs seeking to expand into the US. The working group has been hosted by DOJ and managed by the FBI. It has contributed to the Federal Communications Commission's (the FCC's) "public interest" review of each foreign CSP application by ensuring that the entity adequately assists the investigations of US national security and law enforcement.

Over the past few years, the Trump Administration has grown increasingly concerned about potential threats to the security of America's telecommunications infrastructure.

One sensitive issue is whether to permit Chinese communication service providers to serve the US market. A related question is whether Chinese telecom equipment vendors like Huawei and ZTE pose a threat to our national security.

In response to these concerns, the administration strengthened the review powers of the Committee on Foreign Investment in the US ("CFIUS"). CFIUS performs functions like Team Telecom but spans all industries, not just the communications sector. In addition, last year the FCC opened a rule-making to modify its rules governing subsidies for the buildout of broadband networks in rural areas. The proposed rules would condition the subsidies on the exclusion of Chinese-made network equipment. A few years ago, the FCC opened a proceeding to discuss how to streamline the Team Telecom process. That proceeding may now be moot.

Against this backdrop the President issued the recent EO. Soon, the FCC is expected to finalize its pending rural broadband rule-making in a way that conforms to the EO.

Summary of the EO

The new "Committee" referenced in the title of the EO must be established by July 3rd. It will be chaired by the Attorney General. Other Committee members will include the Department of Defense, the Department of Homeland Security, and other agencies as the President may direct. A secondary governmental group called the "Advisors to the Committee" will play an advisory role in the process. The Advisors will be the State Department, Treasury Department, Commerce Department, the Office of Management and Budget, the Director of National Intelligence, the US Trade Representative, and others.

Upon referral by the FCC, the Committee will review applications filed by CSPs with foreign ownership, as well as the licenses of CSPs that involve foreign ownership, to identify risks to national security and law enforcement. The review process will require the CSP to answer a detailed questionnaire. Presumably, the document will resemble the "triage" questionnaire that Team Telecom routinely handed to foreign-owned CSPs. If the Committee discovers a risk to national security or law enforcement, it may recommend "mitigation" measures to the FCC. Based on those recommendations, the FCC may dismiss the given application, modify it, condition the grant of license on the performance of certain law enforcement assistance, or revoke an existing license.

For example, if the Committee audits a foreign CSP operating in the US and discovers an incident of noncompliance with a license condition, the Committee may recommend that the FCC further modify or revoke the license.

The review process must take place within 120 days of the date the Committee decides the given questionnaire is complete. An additional 90-day period may be used for cases that require deeper analysis. Adverse decisions must be based on a written record. Team Telecom was not required to produce such writings.

Implications for Foreign-Owned CSPs

Foreign-owned CSPs will soon face a more powerful and formal body when seeking FCC licenses to serve the US market. That does not necessarily make it more difficult to enter the US market. Foreign CSPs based in allied nations may jump through the national security hoops just as easily as they did in the Team Telecom days. The new regime will not require foreign CSPs to make any greater commitments to US national security or law enforcement than before. However, if someone as powerful as the Secretary of Defense or Homeland Security deems a CSP suspect for any reason – whether due to the owner's home nation, its ties to suspicious entities, or the nature of the proposed communication service – the official could probably stop the CSP dead in its regulatory tracks.

The Committee's powers appear to be limited. It can only make "recommendations" to the FCC. However, that may be because a more obligatory process would have required Congressional legislation. It is hard to imagine the FCC rejecting a Committee recommendation, especially one backed by the Attorney General. The FCC routinely took the advice of Team Telecom. Based on that record, the word "recommendation" probably means "command."

The national security review process may also become more politicized. For example, if the President needs more leverage in the US-China trade war, he might have his attorney general oppose an FCC application involving a Chinese interest. Alternatively, if the privacy lobby feels aggrieved by a foreign-owned CSP, the group could pressure the Administration – and by implication the Committee – to retaliate using its national security review and audit tools.

In another sense, the higher-profile structure may benefit foreign-owned CSP's. The 120-day review deadline may expedite the license process. Similarly, the more formal rules may create more accountability. A written record of an adverse decision could give

an applicant valuable guidance. In the Team Telecom days, a single review could last a year or more, and the basis for its decisions was never publicly disclosed.

On the other hand, the 120-day process does not start until the Committee chair says the questionnaire is complete. How hard could it be for the chair to find the questionnaire is not complete? That indicates the Committee has flexibility to slow down the train.

By making the national review process more accountable, the EO impliedly makes foreign-owned CSPs more accountable. Applicants must be more candid than ever, in my view, when completing the questionnaire. Beyond that, they must thoroughly implement any promises to assist LEAs. One Committee audit could result in the loss of a license.

The increased importance of CALEA Compliance

The increase in foreign-owned CSP accountability means those entities must, at a minimum, provide good-quality assistance for US lawful surveillance. Specifically, the foreign competitors must be prepared to demonstrate that they can deliver effective interception capabilities as required by the CALEA (lawful surveillance) statute. CALEA differs from the surveillance laws of other nations. For example, under CALEA a court may require a CSP to limit an interception to just the metadata of a suspect's communications. Most of the foreign counterpart laws take an all-or-nothing approach, requiring the disclosure of both content and metadata or nothing at all.

If a foreign CSP lacks familiarity with US surveillance law, it should retain the needed expertise before entering the new Committee-based foreign review process. It may hire a qualified US law firm or a Trusted Third-Party provider of CALEA compliance programs. Subsentio is a leader in CALEA compliance. Either way, the foreign-owned CSP will likely find that US authorities take lawful surveillance more seriously than ever before.