



WHITE PAPER

# Best Practices for Lawful Intercept in Service Providers and Enterprise Networks

Supporting lawful data intercept requests is becoming increasingly important for service providers. At the same time, it has also become a new challenge for enterprises. The world's nations are writing laws legally mandating access to communications, and expanding access to all types of user information including voice, video, data, and even location information. It does not stop there as the requirements and legal application of laws vary by country, and even by state.

This paper provides a basic overview of lawful data intercept, as well as some recommendations for best practices to help you meet basic compliance for several of the mandated lawful intercept scenarios.

## What Is the Problem?

Lawful data intercept is fairly straight forward by definition, but not in application. The simple definition of "lawful data intercept" is the requirement to support a government agency (with an appropriate warrant) in the collection of data communications. That is where the simplicity ends. What you need to support and how you need to support the lawful intercept request depends upon the



The ability to support lawful data intercept is becoming increasingly important for service providers.

government agency requesting the information and your role (and liability) in the delivery mechanism of the communication information.

There are typically four different entities to which lawful intercept requests apply:

- Telephony service providers (wireline, wireless, WiMAX, etc.)
- Internet service providers
- Government agencies (which need to provide information to law enforcement agencies)
- Enterprise and small/medium businesses (including colleges)

Each of these entities has user communication content that can overlap. This includes voice communication, video, instant messaging, facsimile, Internet connections, digital pictures, text messages, data downloads, file transfers, etc. One or more of these content streams could be requested under a lawful intercept order. Depending upon the number of user communication services that an entity provides, it can get very complicated to comply with lawful intercept requests.

For instance, telephony service providers are typically involved with implementing wiretaps for law enforcement agencies. This has traditionally been analog and digital communications, but is converting to packet-based communications for local and long distance communications. In addition, a blurring of the lines between service provider types has become the mainstream. As an example, there are several different service provider types (PSTN, Next Gen Telco, cable TV operator, satellite television, satellite Internet, WiMAX, and wireless (cellular) service operator) that provide Voice over IP (VoIP), video communication, Internet access, business communication services, data storage, cloud services, etc. It is now extremely common for telephony companies to offer IP-based unified communications and other services. Wireless service providers also offer a multitude of unified communications services including voice, video, Internet, data, and location-based services.

Regardless of the communication format or provider, most lawful intercept laws (like CALEA<sup>1</sup> in the USA) demand access to the appropriate content and that access must be provided in real-time. According to the Administrative Office of the United States Courts, which writes an annual wiretap report<sup>2</sup>, there were 3,554 intercept applications submitted by the US federal government or state governments during 2014. In 2015 (the last reporting year), there were 4,148 intercept orders.

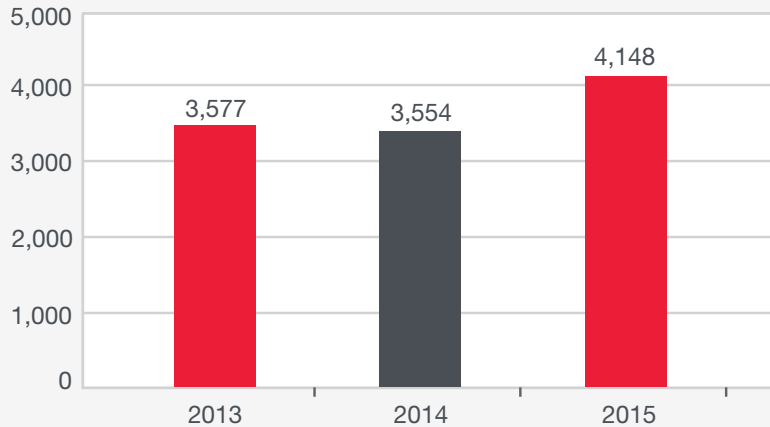


According to the Administrative Office of the United States Courts, which writes an annual wiretap report, there were 4,148 intercept applications submitted by the US federal government or state governments during 2015.

<sup>1</sup> <http://www.fcc.gov/encyclopedia/communications-assistance-law-enforcement-act>

<sup>2</sup> <http://www.uscourts.gov/statistics-reports/wiretap-report-2015>

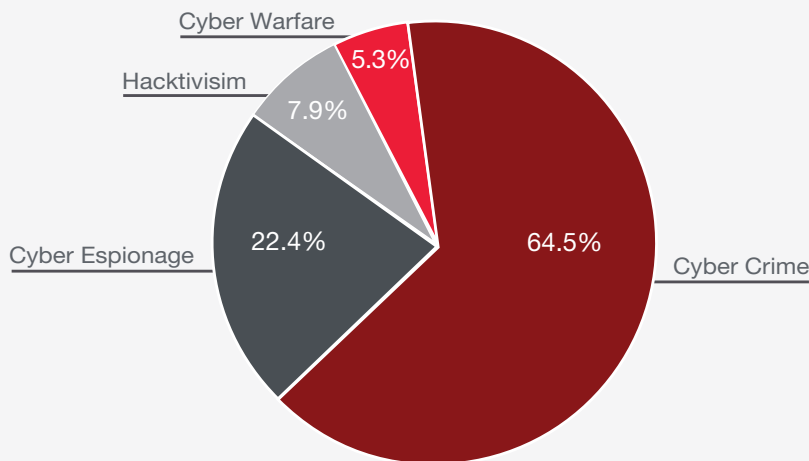
The figure below shows a summary of CALEA requests for the last three years.



CALEA Lawful Intercept Requests (Source: Administrative Office of the US Courts)

We must also remember that the United States has the Foreign Intelligence Surveillance Act (FISA). These warrants come under the CALEA access rules, but do not include the many access needs of our other lesser-known and less-monitored organizations.

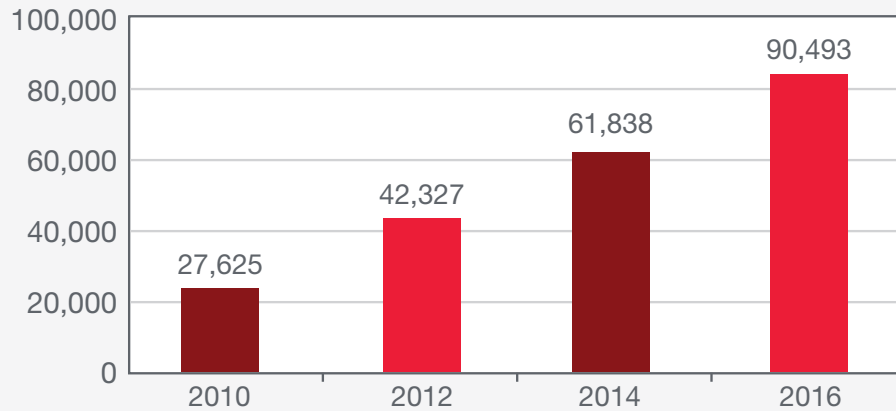
It is also no secret that Internet-related crimes are on the increase. As this type of criminal activity has gone mainstream, the motivations behind it morph as well. Research shows that almost half of hacker attacks are now motivated by criminal intent (fraud, pornography, identity theft, etc.).



### Motivation Behind Attacks Feb. 2017

Hacker Motivation (stats and graphics from Hackmageddon.com)

Should someone think that CALEA only applies to the PSTN or wireless carriers, they would be wrong. Lawful intercept orders are being issued to Internet service providers (ISPs) as well. In fact, the figure below shows that worldwide lawful intercept requests are on the increase for Internet related traffic.



### Google Lawful Intercept Requests

Worldwide Lawful Intercept Requests Made to Google (Source = Google website)

The data in the following chart indicates that the rate of requests to Google continues to increase approximately 20% per year, as law enforcement agencies worldwide focus on combatting cybercrime. One could extrapolate a similar increase for other ISPs.

Year	LI Requests	YoY Increase
2010	27,625	N/A
2011	34,001	18.75%
2012	42,327	19.67%
2013	53,356	20.67%
2014	61,838	13.72%
2015	76,042	18.68%
2016	90,493	15.97%

### Google Lawful Intercept Requests

Made to Google (Source = Google website)

While information about lawful intercept requests to enterprises and small to medium businesses do not really show up in public records, these organizations need to prepare for requests. Not just because of legal reasons but for “personal” reasons as well. Hackers are not just targeting large corporations nor are they just trying to deface websites.

There have been instances where an employee has created an insecure hot spot within a corporate office that a hacker can use for criminal activity. The hacker could sit outside the office in a van on a public street and use the hot spot to gain access to the Internet through the corporate routers. Once on the Internet, the hacker can conduct all sorts of cybercrime (illegal trading, identity theft, cyber espionage, communication with terrorist organizations, child pornography, and the latest craze of Hacktivism for political, social, and religious reasons) that would all be traced back to that particular business (and that particular hot spot) by law enforcement agencies. This could legally incriminate the company and the employee who installed the hot spot. In the end, this behavior could cost both the business and the employee (possibly soon to be ex-employee) lots of time, energy, money, and aggravation to clear their name(s).

In the current era, lawful intercept could potentially become a very serious problem for enterprises. CALEA warrants can be applied to private enterprises, as well as service providers. Bring Your Own Device (BYOD), wireless hotspots, and telecommuting technologies continue to foster a “legal compliance problem” for business leaders and IT, as these applications and technologies can create a representation of a pseudo-ISP. If company resources, networks, or circuits are used for unlawful acts, businesses can be held responsible. In addition, if it can be proved that the IT department and/or executives were aware (or tried not to become aware) that such activities were being conducted by an employee or manager of the company, both the IT personnel and executives can be held liable for complicity – resulting in fines and incarceration for not remediating the commission of those unlawful acts.

Less painful, but not less aggravating, lawful intercept orders may be applied to enterprises for other civil or criminal matters. For instance, in addition to the warrants described above for cybercrimes, access to employee files or communications may be requested in divorce cases or other civil matters.

Enterprises that manufacture communication devices or have data accounts are also being hit with government orders to surrender user information and data. For example, ever since it created the iPhone, Apple has been compelled under USA National Security Letters and the FISA law to surrender data about



CALEA (Communications Assistance for Law Enforcement Act) is the most predominant law in the United States of America.

multiple individuals and accounts. In fact, those user requests are increasing. As enterprises deploy new technologies, they need to be aware of potential implications.<sup>3</sup>

## Short Overview of Lawful Intercept

So, what is lawful intercept? As stated previously, it is the requirement to support a government agency in the collection of communication set-up information and communication content. Most, but not all, countries around the globe have some set of laws authorizing the interception of communications for legal purposes. Some countries (like China) are quite transparent about this interception, while others are not.

We will not review all of the country requirements for lawful intercept, but let us look at a few. CALEA (Communications Assistance for Law Enforcement Act) is the most predominant law in the United States of America. It was enacted in 1994, and complete compliance mandated by 2007, to help clarify what the requirements are for telecommunication service providers in the area of lawful intercept. It was not the first law though. Congress had already passed the Omnibus Crime Control and Safe Streets Act in 1968 to legalize electronic surveillance. Congress followed up in 1970 and then in 1986 with the Electronic Communications Privacy Act, to further strengthen the 1968 law by clarifying that the law extended to telecommunications providers and also went beyond voice communication to include electronic mail, data transmissions, faxes, and pagers.

In 1994, the CALEA law clarified what and how service providers needed to deliver lawful intercept information to US law enforcement agencies. This law was needed to ensure that law enforcement could actually get useful information within a useful timeframe to investigate criminal actions. After the initial law was passed, the Department of Justice and Federal Communications Commission further clarified the law to include packet-based communications and mandated that CALEA must be supported by all service providers.

There were also six other areas clarified to be included as part of the law:

- Content of subject-initiated conference calls
- Party hold, join, drop messages
- Access to subject-initiated dialing and signaling
- In-band and out-of-band signaling (notification message)
- Timing to associate call data to content
- Dialed digit extraction (post-cut-through dialed digits)

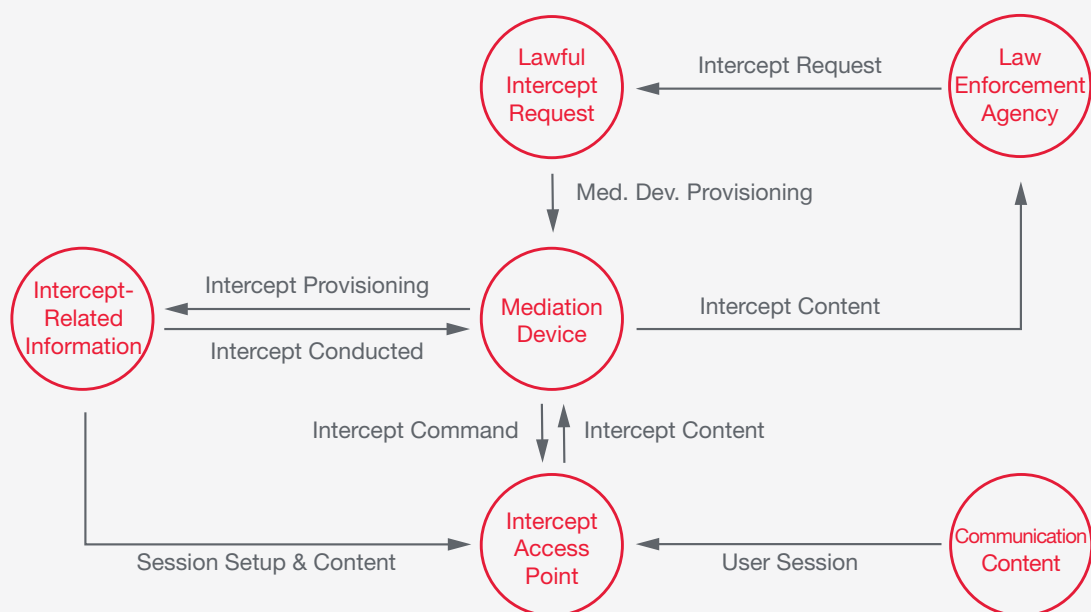


Lawful intercept technically involves several components – wiretapping, pen registers, trap and trace, capturing electronic mail and text messages, capturing images, location information, etc.

<sup>3</sup> <https://threatpost.com/apple-receives-first-national-security-letter-reports-spike-in-requests-for-data/125856/>

The end result was that by mid-2007, all ISPs and communications service providers needed to comply with CALEA. This means that the contents of all communications, along with signaling information associated with the communication, must be captured and sent to the Department of Justice when requested.

Lawful intercept technically involves several components – wiretapping, pen registers, trap and trace, capturing electronic mail and text messages, capturing images, location information, etc. A generic lawful intercept process is illustrated in the following figure. Different nations may adjust the process according to their specific laws.



### Generic Lawful Intercept Process

Many other countries have similar laws to the United States that allow for lawful intercept. Some examples include:

- European Union – European Council Resolution (January 1995) on the Lawful Interception of Telecommunications (Official Journal C 329) and the General Data Protection Regulation of 2016 EU 2016/679 (which is an updated version of the Data Retention Directive approved by the European Parliament and Council in 2006)
- United Kingdom – Regulation of Investigatory Powers Act of 2000
- India – Indian Telegraph Act of 1885, Unlawful Activities (Prevention) Amendment Act of 2004, and Information Technology Amendment Act of 2008. In addition to these three laws, there are additional rules and



regulating bodies involved with lawful intercept and communication surveillance that should be investigated when doing business in this country.

- Canada – Part 6 of the Canadian Criminal Code
- Japan – Act on the Interception of Communications of 1999
- Hong Kong SAR – Interception of Communications Ordinance of 1997/2006
- Australia –Telecommunications (Interception) Act of 1979 and the Surveillance Devices Act of 2004
- Guatemala – Regulations for the Application of the Investigative Technique of Telephone Tapping and Other Forms of Interception of Communications



Organizations must comply with the legal intercept laws or be held accountable.

The 3GPP wireless carrier standard went so far as to directly incorporate lawful intercept capability within it. Those requirements are published as part of the following specifications:

- TS 33.106: 3G Security, Lawful Interception Requirements; which specifies all of the 3GPP requirements
- TS 33.107: 3G Security, Lawful Interception Architecture and Functions; which includes the functional architectures for 3GPP services
- TS 33.108: 3G Security, Handover Interface for Lawful Interception; which specifies the Handover Interface between the service and the LEA

In the United States other federal laws, such as the Foreign Intelligence Surveillance Act of 1978, the PATRIOT Act of 2001, and a renewal of the expired parts of the Patriot Act (now called the USA Freedom Act of 2015), provide additional guidance on lawful intercept of communications – especially with respect to foreign suspects and potential terrorist threats. Other countries also have laws that expand their lawful intercept practices in situations of suspected terrorism and/or in regards to terrorist organizations.

## Common Implementation for Lawful Intercept Monitoring

Now that we have explained what lawful interception is and why it has to be supported, this section contains an overview of how to implement it.

Organizations must comply with the legal intercept laws or be held accountable.

When faced with a lawful intercept order, an entity (whether it is a service provider, ISP, government agency, or private enterprise) has one of four options:

1. Do not comply. In the case of CALEA, this will typically result in fines of up to \$10,000 per day and possible arrest of anyone within the organization failing to implement the court order. Laws in other countries are similar.



2. Install the technology. Integrate the technology required for lawful intercept and perform the actions authorized by the court order.
3. Obtain third party services. Hire a trusted 3rd party (that is legally authorized) to perform the activities requested under the court order.
4. Close down the entity. Law enforcement officials will still demand access to equipment and records acquired up to the point of closure, and possible criminal actions can be sought against the managerial leadership of the entity closing down, depending upon their relationship to the suspect identified in the court order.


For the purposes of this paper, we will focus on options 2 and 3 above. In regards to option 2, the first question you will need to answer is what are you required to deliver to law enforcement agencies (LEA)? There are usually two different responses. The first method is a complete copy of all your traffic. Sometimes referred to as “The PRISM Project” in the United States, this is in fact a basket full of programs for both foreign and domestic intelligence agencies, and covers all types of communication – cellphone, radio, satellite, data, etc. PRISM uses very high-end algorithmic search sequences, key words, methods, encryptions, hidden file types like stenography under the SIGINT (Signal Intelligence) methods, or alphanumeric designation formats. The LEA can then take the traffic and filter to find what they need to fulfill the warrant or intelligence need. This basic request is more commonly issued to ISPs.

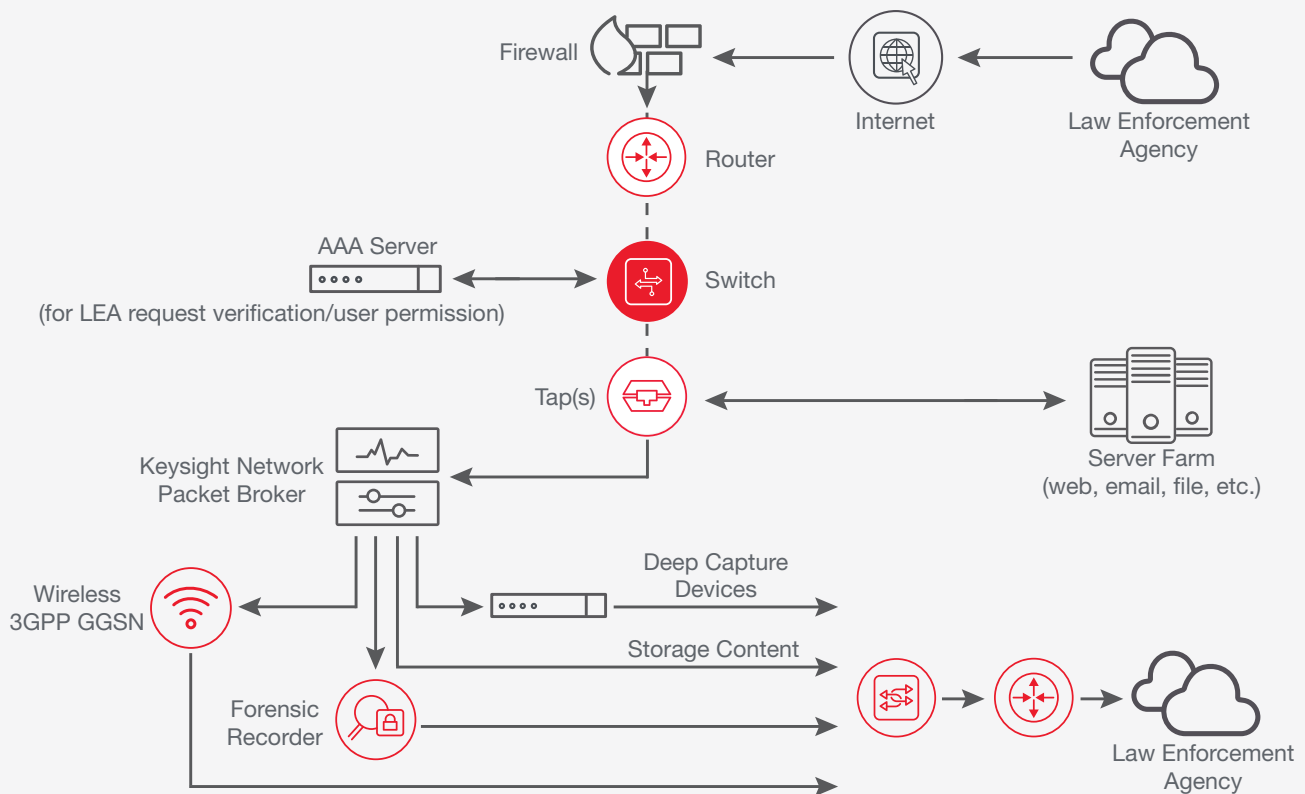
The second method is for the entity to filter their complete traffic to get only the relevant pieces of information sought in the warrant, and then provide that information to the LEA. The courts in various countries (like the United States) are very sensitive to “fishing events” and the requesting legal agency must have good cause for gathering the information – or the order must come from the Intelligence Oversight Court. The courts do NOT allow fishing expeditions, so there must be a very specific reason for a CALEA warrant, and in many cases local and state warrants must be issued and aligned with the Federal warrant. The relevant information depends upon the court order. It might only be the envelope information (IP addresses involved, etc.) but not the actual contents of the message itself. Or, the court order may specify both pieces.

When beginning to implement the second method, the first question for IT to ask is where to capture the information within your network (e.g. from a Switched Port Analyzer [SPAN] or a tap). The cloud can make warrants very difficult, as connection points and the data (evidence) may lie in different countries. Due to potential latency issues, timing errors, and packet loss with a SPAN, you should try to access the information from a tap to eliminate latency and loss problems in order to get every bit of the data. The taps can be applied either inline or out-of-band, depending upon the application needed.

However this connection is made, it should be unknown to the suspect so that they have no knowledge of the “wiretap.” This, again, is subject to the prevailing local, state, and country laws, as well as warrant type.

The next question is how to capture the information. You will want to use a filtering device to capture and filter the data to get the required information so that you can aggregate and segment the necessary data. A network packet broker (NPB) contains the ability to deduplicate unnecessary data, create detailed filtering rules to segment data packets, provide the necessary aggregation of the appropriate lawful intercept data required, and then finally send it downstream to the appropriate collection point for the LEA. The right monitoring switch can process the data at line rate and eliminate concerns of tainted evidence. The filtering device should be a firmware based device, not a SPAN. Without a filtering device, lawful intercept will become an expensive and painful activity for you as you try to separate the relevant and non-relevant packet data with other devices. The following diagram shows a brief overview of lawful intercept filtering:

 When beginning to implement the second method, the first question for IT to ask is where to capture the information within your network (i.e., from a SPAN or a tap).



### Lawful Intercept Monitoring

The last point to consider is your mechanism to ensure that the chain of evidence is secure. You will normally be legally required to prove that the evidence collected was not tampered with and was kept confidential. Any break in the chain of evidence can create testimony issues and challenges. One lost frame, or even a questioned frame, can lose a case due to reasonable doubt.



The chain of evidence can be broken in several places including the following:

- Captured data is sent to the wrong location (port)
- Some of the captured data is lost (as with a SPAN port)
- There is a “significant” time delay in the forwarding of the required information
- Captured data includes other non-relevant data (i.e. packets)
- Transport protocol or method contamination

It is your responsibility to address these concerns within your network. Remember, you may need to explain the data capture process you used in a court of law, and explain to a jury why it was captured that way. If there is ANY doubt as to the reliability of the data, the typical rule of law (depending upon country) is that the evidence must be suppressed or the charges must be dismissed. If further evidence is based on the data gathered and there is a question as to its validity, then all other evidence from that must be struck. This is called “the fruit of the poisonous tree,” or “poison root/poison fruit exclusionary rule.” More information on this topic is available from Wikipedia at “fruit of the poisonous tree.”<sup>4</sup>



**Any break in the chain of evidence can create testimony issues and challenges.**

For option 3 above, a trusted third party may be used as a contractor to perform legal intercept activities for any organization needing such services. In the United States, the FCC proposes to allow third parties to manage government surveillance requests. The private company would analyze all the data from a telecommunications carrier, extract information relevant to the court order, and send it to law enforcement. They, for a fee, put in the appliance for their customers. When a warrant is issued, that trusted third party comes in and builds the access portal with the required filtering. They typically charge by the day, the amount of data, and by the hour of setup and tear down.

Privatizing this traditionally government function may have ramifications to the entity served with the court order, as well as the third party. There is no assurance that third party entities will safeguard the privacy and security of information not authorized to be collected. So, they may collect far more data

---

<sup>4</sup> [http://en.wikipedia.org/wiki/Fruit\\_of\\_the\\_poisonous\\_tree](http://en.wikipedia.org/wiki/Fruit_of_the_poisonous_tree)

than required, and that data may be something that the customer employing them does not want to “leave the building.”

For example, a contracted company could perform a legal intercept service which requires the providers to pipe all of their data to the contractor. Then the contractor’s employees analyze the data, extract information relevant to the court order, and send it to law enforcement. This transaction leaves personal data potentially vulnerable when it travels from the service provider’s network to the contractor’s network. It also places the personal data of innocent people in the hands of a third party without customer consent. It is unclear how these “trusted third parties” can be effectively monitored to protect your communications. If too much information is collected, will you know about it? More generally, there could be privacy consequences to the entity employing trusted third party services. New laws, like the General Data Protection Regulation (GDPR) law, need to be investigated to see if there are any implications for data privacy when using third parties.



## Best Practice Recommendations for Monitoring and Lawful Intercept

Keysight has gathered extensive knowledge over several years on how to properly filter packet data for private enterprise, service providers, and government agencies. Based upon this knowledge base, we offer the following recommendations in regards to lawful intercept:

- Use taps, not SPANs, as the information collection point
- Install proper filtering to capture the necessary content quickly and easily
- Address your equipment security concerns upfront
- Make sure you protect the captured evidence

### Use taps, not SPANs

While both SPANs and taps can be used to provide lawful intercept information to a monitoring switch, taps are the superior equipment to use. SPANs, by their nature, can limit the information that is passed on to the monitoring switch. Taps are completely passive and do not limit or consolidate any of the information. Everything is forwarded downstream.

At the same time, the information passed on by the SPAN will probably be delayed due to the internal processing of the information by the SPAN device. This means that you will not be getting a true representation of the network.



While both SPANs and taps can be used to provide lawful intercept information to a monitoring switch, taps are the superior equipment to use.

This delay can affect time stamping information related to the lawful intercept content as well as a delay of the actual information to the LEA. The time delay effects become more noticeable as data rate speeds reach 10GE and beyond.

Security of the information is another concern, as SPANs typically have the ability for external management (and therefore external security risks) that a passive tap will not have. Taps are not addressable network devices, so they cannot be hacked like most SPANs (which have remote management capabilities). Because of the three concerns above, data captured for the LEA using a SPAN has been challenged in courts of law and thrown out in some cases.

Use of VLAN access control lists (VACLs) are discouraged as well. While these can be used like SPANs to forward certain types of traffic, they have timing and reliability issues like the SPAN ports we just discussed. In addition, they require more programming effort, introduce more complexity into your network, and may have IPv6 support limitations. A tap will provide superior performance at a much lower cost.

## Use a network packet broker

Using a network packet broker will make complying with legal intercept laws a lot easier. One benefit is that intercept requests can be made without change board approvals to interconnect monitoring tools and connection setups for the lawful intercept. When a request is made the IT department can quickly provision circuits and routes without any executive approvals, and without any impacts to the production network.

A second benefit of packet brokers is that they make data filtering setup extremely easy. Manufacturers (like Keysight) allow the IT department to filter between ingress and egress points based upon extensive criteria, which allows only specific packet data to be forwarded in compliance with lawful intercept requirements.

In addition, there are three more benefits from using an NPB:

- Traffic aggregation from multiple links
- Load balancing and rebalancing to eliminate traffic overload downstream
- Remove various packet labels (like GTP and MPLS) that lawful interception probes cannot understand

Another important aspect is the filter maps. You may be asked to explain how the monitoring switch filters work, what criteria is being screened along with how the filters are connected, and what they are connected to (e.g., which ports, tools, etc.). Having an NPB with an accurate, easy-to-read, easy-to-explain visual map of the intercept will be easier for a jury to understand. That in turn makes your life easier. In fact, if you print the maps out, they could be self-explanatory. The alternative approach would be to print out command line tables which would definitely have to be explained at length, and could be picked apart by defense attorneys. GUI interfaces are the easiest to explain and cannot be as easily challenged as command line filters. While nothing here is intended as legal advice, keep in mind that you may be required to explain the access method and filtering rules you implement to a court room jury.

## Address security issues

Security is a major concern. As mentioned earlier with the SPAN device discussion, network security must be addressed for all components in your network that are used for lawful intercept. Any access device can be called into question in civil and criminal cases over security and access concerns.

Threat vectors are constantly changing and network operators should be constantly verifying their network security. One well known threat vector is to spoof an SNMPv3 (any version actually) Interception Request. This vector can allow a hacker to redirect lawful intercept information to a non-authorized entity. In addition, Cisco published a lawful intercept implementation model in the IETF document RFC 3414. This and other models can be vulnerable to other attack vectors like using Brute Force attacks on SNMPv3. For more information on these security vulnerabilities, consult the paper “Exploiting Lawful Intercept to Wiretap the Internet,” written by Tom Cross.<sup>5</sup>

Investigation for lawful intercept threat vectors should augment your traditional threat assessments and persistent threat parameters as well. For instance, the use of Trivial File Transfer Protocol (TFTP) and other protocols could give hackers access to some of your servers which would allow the access to routing tables and access lists that could be used as a stepping stone to target their main objectives. Also, access can turn servers into rogue “bot” servers that attack other companies, governments, organizations, etc.

Access to lawful intercept components and activities should be limited within your organization. Physical access to equipment is one aspect. Another component includes role-based access to your packet broker, as well as

---

<sup>5</sup> [http://www.blackhat.com/presentations/bh-dc-10/Cross\\_Tom/BlackHat-DC-2010-Cross-Attacking-Lawfull-Intercept-wp.pdf](http://www.blackhat.com/presentations/bh-dc-10/Cross_Tom/BlackHat-DC-2010-Cross-Attacking-Lawfull-Intercept-wp.pdf)

granular permissions with respect to creating and modifying any lawful intercept filters that you set up so that others cannot accidentally (or deliberately) modify those filters.

Permissions and authentication controls may also require the use/connection to an authentication, authorization, and accounting (AAA) server. This depends upon the type of intercept access point (IAP) that is being used by the lawful intercept agency. LEA requests should be authenticated in some manner to verify that the request is authorized, and also to capture the intercept-related information (e.g. the target's username and system IP address) for the intercept request. The intercept-related information can be used by a service provider to determine which equipment (a router) that lawful intercept target's traffic is passing through.

Proactive action with respect to security will eliminate future problems and headaches for you.

## Protect the chain of evidence

As mentioned previously, the chain of evidence must be preserved. This is typically mandated by government laws on legal intercept. It does no good for the law enforcement agency to receive incriminating information on suspects when that data will be challenged and dismissed in court proceedings.

There are some basic things that the IT department can do to protect the evidence:

- Provide only the evidence specifically requested in the warrant – an approach of providing everything possible is a poor approach that could actually “contaminate” good data
- Separate the data for each warrant – if more than one warrant is received at a time, correlate the specific content for each warrant rather than combining multiple streams of information and intermingling the content of different wiretaps
- Show other access, hyperlinks or redirections used by a suspect separately to the LEA
- Collect tracking and location information separately. Depending on the prevailing law, separate warrants may be required for the different sets of information.
- Prevent the loss of the lawful intercept data within your network
- Periodically validate your collection and delivery processes to ensure that they are correct, particularly your routing and storage paths



Examples of information to collect include: time (start/finish/break), methods (of access, filtering, storage), reasons for access and or monitoring (including deep storage), items discovered, all server logs saved, and other items.



- Maintain intercept log books to keep up with any activities associated with the wiretaps – this includes logs of who has access to any and all parts of the access technology, written and saved logs of setups and procedures used, and details about all the warrants or routine monitoring.

In regards to log books, this simple task can go very far to demonstrating your company's due diligence in collecting and protecting the chain of evidence. Examples of information to collect include: time (start/finish/break), methods (of access, filtering, storage), reasons for access and or monitoring (including deep storage), items discovered, all server logs saved, and other items. Everything that is saved should be stored in a special place, with as much protection as possible – including all physical logs on suspect building info, videos, RFID logs, etc. These processes should be the same for all evidence gathering – civil, internal violations, and policy violations (including criminal). Access to the log books and files should be limited as well.

With respect to routing and storage paths, a simple activity is to periodically check that your routing tables and access lists are correct. Since modern data networks are often in a state of flux, it becomes easy for routing tables and access lists to contain errors that can cause multiple routing problems. For lawful intercepts, you need to validate that the information is going only where it should. IT should always have a network map.

This includes all wireless points (which should be mapped and protected), and no BYOD wireless access points should be allowed. Another best practice is that passwords and physical credentials should reflect the actual user, not a group. Direct access and filtering technology should also be password protected and physically isolated and locked, if possible.



**Lawful intercept applicability and responsibilities are expanding far into the data world.**

## Conclusion

Lawful intercept applicability and responsibilities are expanding far into the data world. All service providers are directly affected by international laws governing this area. Private businesses can be affected as well. Many have already found that they too can be issued warrants for monitoring. To protect your interests, there are several best practices that you can employ to make compliance with these laws less stressful for your organization:

- Deploying Keysight taps and network packet brokers for selected visualization are an efficient and easy way to help you support those lawful intercept requests – not to mention your own analysis, monitoring, compliance and auditing demands.
- A network packet broker gives you the capability to divert relevant information to the right monitoring tool at the right time for the correct purpose. The Keysight Vision ONE network packet broker product is quick and efficient for all entities (traditional telephony service provider, Internet service provider, government agency or enterprise) to deploy to meet your filtering obligations.
- An NPB also provides traffic aggregation, load balancing, and header stripping to further make your life easier when complying to a lawful intercept request
- A security-related best practice recommendation is to periodically validate your network security, especially as it applies to lawful intercepts. This assessment includes hacker accessibility (through SNMP, FTP, etc.) and the use of role-based permissions.
- A final best practice is to ensure that your lawful intercept policies and procedures address protecting the chain of evidence. IT needs policies, practices and procedures for lawful intercept as well as for their everyday monitoring, auditing, security compliance and scans, analysis, server access studies, etc., plus a list of who has access to what and how.

Learn more at: [www.keysight.com](http://www.keysight.com)

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: [www.keysight.com/find/contactus](http://www.keysight.com/find/contactus)

