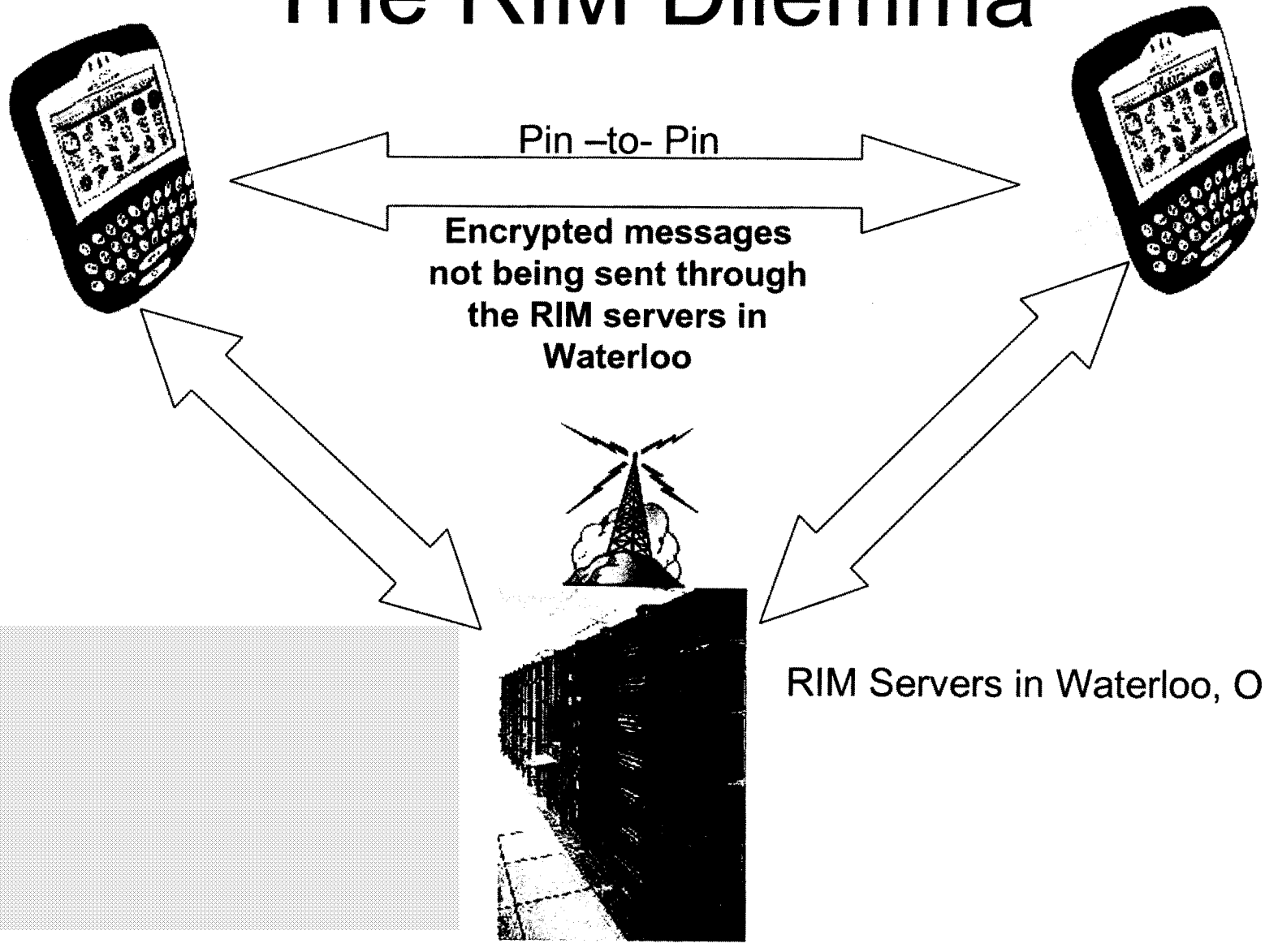
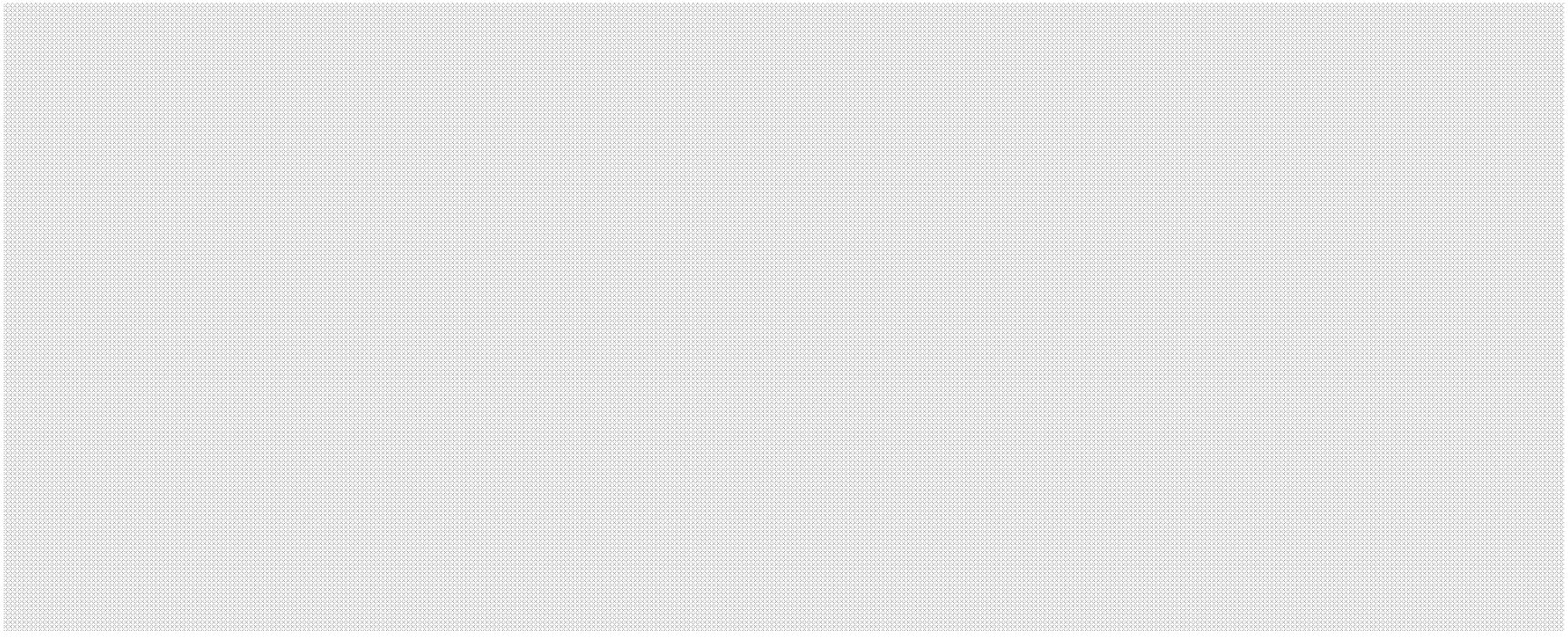
The RIM Dilemma



s.21(1)(a)
s.21(1)(b)

Alternative Techniques

- According to the Performance Measurement Framework. The RCMP and CSIS with Support from the CSE have developed new;



Tariff rates for hook-up in other countries

[redacted] However, for your information we include brief analysis from the U.K., Australia and New Zealand.

United States (1995)
***Communications Assistance for Law Enforcement Act* (CALEA),**

In the U.S, hook-up fees vary widely. A hook-up to a network that is CALEA compliant costs law enforcement on average $2,200, with some carriers charging as low as $250 and others charging as high as $3100. However, these costs might be inflated because investigators from the U.S. justice department are unable to determine if the carriers are passing capital costs on to law enforcement. TSP fees are also inconsistent charging different prices to different law enforcement agencies and differing by state.

We must note that pre-CALEA network upgrades were paid for by the FBI which was granted $500 million for modifying systems installed or deployed prior to the coming into affect of CALEA on January 1, 1995.

[redacted]

United Kingdom (2000)
***Regulation of Investigatory Powers Act* (RIPA)**

Any Communication Service Provider, such as a public telecommunications operator, postal carrier, Internet service provider or international simple voice resale provider is covered by RIPA. The cost burden on the telecoms industry of implementing the new measures has been substantial. RIPA imposes a duty on the Secretary of State to ensure that a service provider receives a "fair contribution" towards the cost of complying with an interception warrant or maintaining intercept capability.

A sum of £20 million was earmarked for communications provider support for the three years from 2001 to 2004 in connection with broader RIPA obligations, of which £14 million was spent in the first year. Further consultations are taking place between the Government, industry and the TAB on the precise costs to the industry of complying.

Australia (1979)
Telecommunications (Interception) Act

Telecommunications interception legislation is "designed to be technology-neutral and applies to any form of communication - voice, fax, images or data - passing over a telecommunications system. Specifically, Part 15 of the Telecommunications Act 1997 obligates carriage service providers (inc. ISPs) to ensure that their network is able to intercept a communication passing over it in accordance with a warrant issued under the Telecommunications (Interception) Act 1979.

For telecommunications carriers, the Bill stipulates that they must meet the costs of developing, installing and maintaining interception and delivery capabilities. However, carriers are still paid for what we would define as "Hook-Up". According to the Australian Attorney General, total costs of interception per warrant ranges from AUS $4,700 to $22,953 of which "Hook-up" fees are included. As of October 22nd, 2007 $1.16 AUS = $1.00 CDN.

New Zealand 2004
Telecommunications Interception Capability Act.

In November 2004, New Zealand passed the *Telecommunications (Interception Capability) Act.* It requires network operators to ensure an interception capability of telecommunications networks and services.

Costs
The government will pay $3M towards the provision of interception capability for existing fixed and mobile voice networks to be implemented within 18 months from the date the legislation is enacted.

ISPs will have to pay for the cost of upgrading their Internet and email services.

ISPs have been given five years to implement the changes needed to meet the requirements of the new law.

Information directly regarding "Hook-up" in NZ wasn't available.

procera NETWORKS

CALEA Compliance

The Way Forward

Procera Networks is a pioneering, global developer of intelligent network traffic identification, control and service management infrastructure equipment. Procera's PacketLogic product line was purpose built for ISPs and Broadband Service Providers as a flow-based intelligent network traffic and service management system.

The core of the product suite functionality is DRDL™ (Datastream Recognition Definition Language) that provides the most accurate network traffic identification available today. PacketLogic solutions are currently deployed at more than 200 Internet Service Providers, and over 375 sites worldwide.

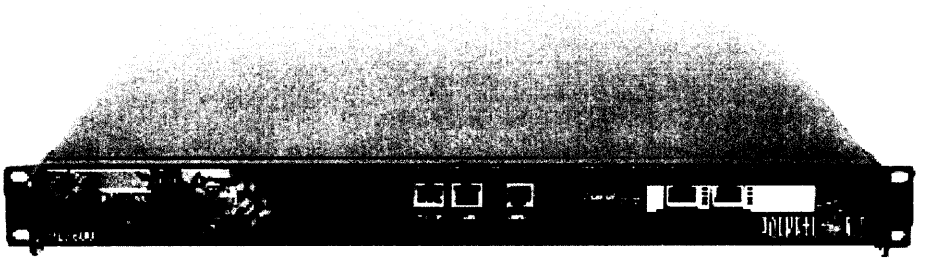
CALEA Compliance – the Way Forward ...

Executive Summary

The FCC has set a firm deadline of May 14, 2007 for all Internet access service providers and VoIP Interconnect service providers (collectively referred to as BroadBand Service Providers, BSPs) to achieve compliance to the CALEA regulations. They will need to upgrade their networks to provide law enforcement agencies access to wiretaps on IP networks for data and voice communications. Given the proliferation of mechanisms of compliance–ranging from complete outsourcing to partial outsourcing of the CALEA technical solution to a trusted third party (TTP) to implementing the technical solution in house–it is critical that small and medium service providers choose a solution that works, addresses their business and technology challenges today, and can be easily upgraded to address future changes in the regulations.

Procera Networks' offers the PacketLogic platform, a cost effective, complete, and scalable solution that seamlessly integrates into the service provider's existing network, without the need to upgrade any network element in the network infrastructure fabric. Procera's unique value proposition is that in addition to being able to handle the Interception and Delivery of content as sanctioned by the FCC CALEA regulations, the solution also delivers the most accurate, policy-based traffic management capabilities for Broadband Service Providers (BSPs).

In this paper we examine the cost benefits of the possible implementation models with Procera Networks' PacketLogic platform, and details how you can achieve CALEA compliance within the deadline and your cost targets.



PacketLogic

Introduction

Effective May 14, 2007, all BSPs need to be compliant to CALEA (Communications Assistance for Law Enforcement Act). Compliance requires BSPs to transfer a 'target' subscriber's communications to the authorized law enforcement agency (LEA) in real time. This white paper examines:

- CALEA Requirements
- The Challenges
- CALEA Implementation Models
- PacketLogic—The CALEA Solution
- PacketLogic Technology
- Comparative Costs of Implementation Models
- Advantages of Procera Networks' PacketLogic-based Solution

Note: You may sign up for webinars on this topic on our website www.proceranetworks.com. PacketLogic is a ready-to-use tool and is currently deployed at over 300 broadband service provider facilities.

CALEA Requirements

When an electronic intercept is legally authorized, LEAs may require two categories of information-Call Identifying Information (CII) and Call Content (CC)-to and from a particular target. The warrant is very specific about the types of data traffic to be captured and delivered to the LEA. The BSP must capture the warranted information and redirect it to the LEA for real-time analysis.

Refer to **Appendix B** for understanding the process in detail.

Procera provides the technology that enables BSPs to achieve technical compliance with CALEA. This requires an interception and a delivery process, which involves a 2-way communication between the service provider, (or a proxy—trusted third party), and the LEA. Respective responsibilities and the process are outlined in the illustration and the table below.*

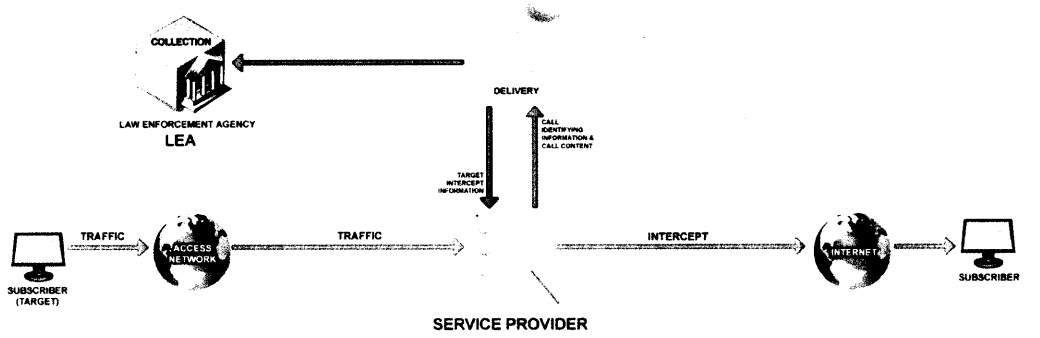


Figure 1: The CALEA Process

* The FCC regulations state that the BSP must document policies and procedures on how to Intercept and Deliver communications from a target subscriber, when served with a warrant. The BSP must file these policies and procedures with the FCC.

Table 1: CALEA Responsibilities

Service provider	**Administration**	**Provisions intercepts; interfaces with LEA(s)**
Service provider	**Interception & Extraction**	**Isolates, intercepts and extracts all CII and CC in a non-industry specified format; and transfers it to LEA via an industry specified format or a mediation device**
Service provider	**Mediation & Delivery**	**Receives intercepted information from the interception device in a non-industry specified format and formats it into an industry specified format and delivers it to LEA(s); maintains confidentiality across multiple flows to LEAs, if they exist**
LEA	**Collection**	Collects, stores, and analyzes intercepted information

Note: The FCC allows service providers to engage trusted third party compliance providers to provide technical assistance to LEA by providing CII and/or CC on behalf of the service provider. **However, the legal responsibility still resides with the service provider.**

The Challenges

Service providers need a solution that:

- Tracks all known protocols for identifying voice and data calls on the IP network
- Isolates, intercepts, extracts, exports CII and/or CC at packet level for a legally identified target suspect on the service provider's network to the LEA

The solution also needs to address the following business and technology challenges.

Business Challenges

- Address privacy concerns of subscribers
- Intercept and deliver only warranted information
- Provide optimum performance to subscribers
- Maintain anonymity/transparency of intercept actions
- Provide flexibility and scalability to meet BSP's growth
- Minimize manpower costs for operations and implementation of CALEA technical assistance
- Keep initial capital expense and ongoing operational costs low
- Minimize or eliminate interruption to BSP's network and/or workload when a warrant is received

Technology Challenges

- Seamless integration into the existing network
- Maintain network performance
- Address security concerns of the network and users
- Provide flexibility and scalability to meet future enhancements to CALEA regulations
- Handle new and emerging voice and data protocols and services

CALEA Implementation Models

Three CALEA implementation models have emerged that service providers can choose from. These are:

- **BSP interacts directly with the LEA by provisioning interception and delivery technology in-house.**
  Costs vs. benefits:
  Upfront capital costs due to additional equipment and trained manpower requirements. But these are offset by the business and technology benefits such as subscriber privacy, network security - and in one case by the inclusion of network traffic analysis and management capabilities for general commercial benefits as part of the CALEA solution. Initial capital expenditure is medium to high, but ongoing running costs will be low.

- **BSP works with a trusted third party provider (TTP) on a 'turnkey' basis.**
  Costs vs. benefits:
  Upfront costs are fixed—start up fees plus recurring monthly fee and per warrant incident fees. Vendor fee structures and network deployment models vary widely. Business and technology advantages may not accrue. The TTP may still require upgrade of network infrastructure routers with special software or other equipment so there maybe additional capital costs resulting in higher total long term costs.

- **BSP provisions interception and outsources delivery.**
  Costs vs. benefits:
  This approach incurs upfront capital costs plus some recurring operational costs. Most BSPs will require upfront costs of upgrading network infrastructure router software and potentially some passive probes. Cost can be medium to high for the upgrade and third party services; operating costs are variable, but margins will reduce. Business and technology advantages may also not accrue.

BSPs may choose an implementation model depending on the scale of their business and their cost structure. However, they need to ensure that the technology underlying the chosen model must be extremely robust and scalable to address the business and technology challenges, and to ensure the ability to keep up with future changes in the interception specifications.

PacketLogic—The CALEA Solution

Procera Networks offers a cost effective, easy-to-implement platform—PacketLogic™ Lawful Intercept Rules system (PLIR), which supports all the implementation models for BSPs and trusted third party providers.

PacketLogic is a flow-based traffic management system. It addresses the problems of service providers to isolate, intercept, extract, export, and selectively monitor in real-time a legally identified target subscriber on the BSP's network, without compromising the constitutional right to privacy for the rest of the subscribers on the network, or comprising the performance of the network for either the suspect or the rest of the subscribers.

The illustration below depicts Procera's CALEA solution—PacketLogic Lawful Interception Rules system (PLIR) and the PacketLogic Lawful Inspection Delivery (PLID) system. The PLIR handles the interception and extraction of suspect data while the PLID provides the mediation and delivery of the suspect data to the LEA.

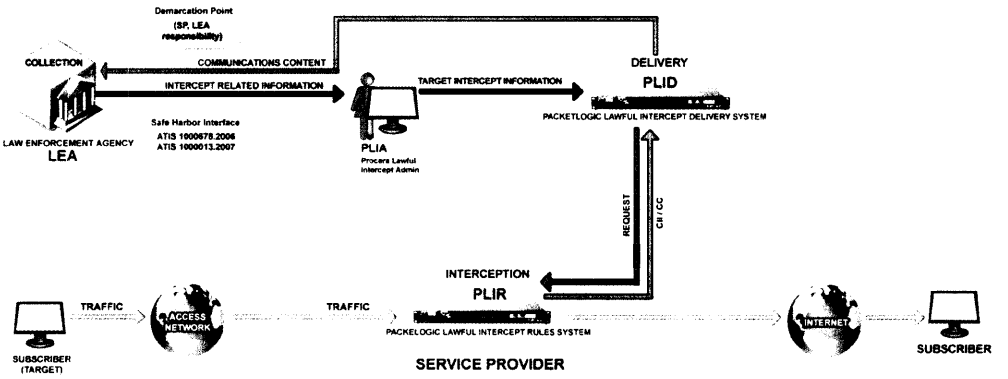


Figure 2: The PacketLogic CALEA Solution

The PacketLogic solution works well in the scenarios described earlier as implementation models.

Scenario 1: BSP Owns Interception and Delivery

The PacketLogic platform is deployed in the BSP's network infrastructure. The illustration in Figure 2 depicts the deployment and meets all the business and technology challenges such as keeping initial capital expenditure and ongoing operational costs low, maintaining subscriber privacy and network security. An added benefit for service providers is PacketLogic's traffic management capabilities that enable BSPs to manage their networks for getting better network performance and increased Quality of Service, as well as respond to LEA requests.

Scenario 2: BSP Outsources Interception and Delivery to a Third Party

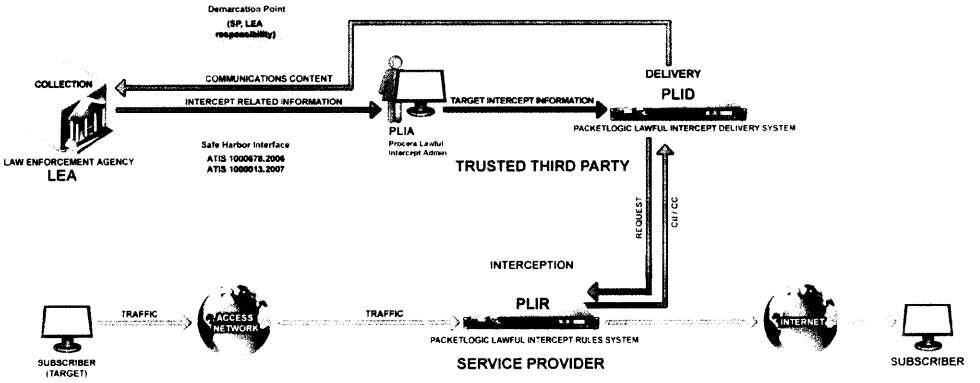


Figure 3: BSP Outsources Interception and Delivery to a TTP

In this case, the TTP installs the PacketLogic platform in the service provider's premises and administers the legal intercept (LI) system from a central location for a number of such clients. The BSP will be able to use PacketLogic's traffic management capabilities for defining and extracting the warrant specific CII and/or CC.

Note: In this scenario, the BSP will not be able to use the traffic shaping and filtering capability of PacketLogic for other purposes. However, The TTP may be able to offer traffic management services for applications other than Lawful Intercept.

Scenario 3: BSP Owns Interception and Outsources Delivery to a Third Party

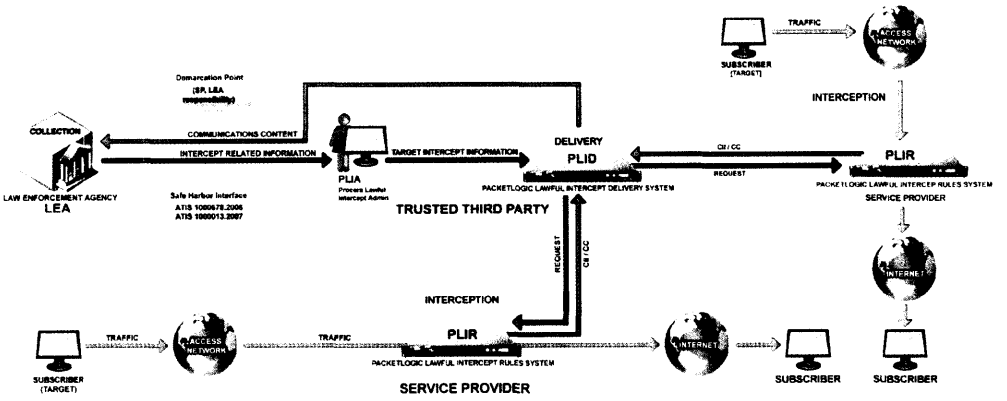


Figure 4: TTP Manages Delivery for Multiple Service Providers

This scenario can also be implemented very successfully—where a service provider had deployed a PLIR for traffic management and then engages with a TTP using a PLID for delivery to LEA. Since both the inspection and the delivery systems are from Procera, this scenario provides yet another option for the service provider to comply with the CALEA regulations.

PacketLogic Technology

PacketLogic is an ideal CALEA solution due to the extended deep flow inspection technology (DFI) that Procera Networks uses to identify services and hosts in a network. PacketLogic uses it's highly optimized traffic analysis engine (DRDL - Datastream Recognition Definition Language) to identify applications independent of the network ports to deliver a very accurate and scalable traffic management solution. Because DRDL is the most accurate traffic identification technology, it also makes it the best "forensics engine" for the lawful intercept applications.

Highlights of the technology are:

- Identifies packet flows and connection flows simultaneously and places them in a contextual relationship to track control and data sessions
- Tracks connection flows to track packet flows—even if certain protocols port hop
- Flows are viewed bi-directionally—essential for accurate tracking of communications flows
- Tracks encrypted traffic such as SSH and Skype
- Integrates seamlessly into the BSP's network infrastructure without requiring any changes or upgrades to existing network elements
- Provides traffic management capabilities
- Imposes no requirements on the network infrastructure fabric since PacketLogic is an optimized passive appliance and sits on the edge of the networ
- Utilizes a signature database of all common services used by applications

More than 300 application protocols (HTTP, SMPT, FTP, Kazaa, Direct Connect, SSL, SSH, Skype) are identified using DRDL and new signatures are constantly added. It's also possible to script signatures to identify proprietary applications.

Note: Besides CALEA, PacketLogic is extensible to comply with other regulations such as those prevalent in the European Union.

Comparative Costs of Implementation Models

Procera technology can be used to implement any of the three scenarios mentioned earlier. However each scenario has a different cost structure in terms of initial capital expenditure and ongoing variable costs. The table below compares the various costs that the BSP should consider when considering each of the solution models with or without Procera supplied equipment..

Table 2: Costs Incurred for Implementing Models using Procera Equipment vs. Other Equipment

	Type of Cost	Interception Equipment	Mediation & Delivery Equipment	Monthly Service Cost	Per Intercept Cost	Remarks
BSP owns Interception & Delivery (using Procera equipment)	Fixed	Low	**High**	None	None	Only fixed costs for PacketLogic equipment, with no recurring costs
	Variable	None	None	None	None	
BSP owns Interception & Delivery (using other vendors' equipment)	Fixed	**High Cost of upgrading switches and routers**	**High one time purchase price**	None	None	High fixed costs with no recurring costs
	Variable	None	None	None	None	
BSP works with a TTP on turn key basis (TTP uses Procera equipment)	Fixed	None	None	None	None	No fixed costs but low-medium variable costs
	Variable	Low	Medium	Medium	Medium	
BSP works with a TTP on turn key basis (TTP uses other vendors' equipment)	Fixed	None	None	None	None	No fixed costs but medium-high variable costs
	Variable	**High Lease or installation fee**	**High One time sign up fee, varies by network**	**High cost per subscriber**	Medium	
BSP owns Interception & engages TTP for Delivery (BSP and TTP both use Procera equipment)	Fixed	Low	None	None	None	Low fixed costs and low variable costs
	Variable	None	Low	**Low**	**Low**	
BSP owns Interception & engages TTP for Delivery (both use interception and mediation equipment from other vendors)	Fixed	**High Cost of upgrading switches and routers**	None	None	None	High fixed costs for equipment and trusted third party fees; and recurring fixed costs and high variable costs
	Variable	None	**High One time sign up fee, varies by network**	**High cost per subscriber**	**High**	

Advantages of Procera's PacketLogic-based Solution

Procera's PacketLogic solution meets all the challenges mentioned earlier, including business and technology.

Table 3: Advantages of PacketLogic Solution

CALEA inspection and delivery tool	Provisions lawful intercepts (along with LI administration) and handles delivery; tracks all known protocols for identifying IP voice and data communications on the network; can conduct multiple and concurrent LI on the same or different targets
Privacy	Since interception and delivery use proprietary encrypted protocols for communication, subscriber privacy is maintained
Warranted information	Intercepts CII and/or CC only for suspect subscribers by implementing very precise extraction rules; the interaction between PLIA(Procera Legal Intercept Admin), interception, and delivery is automated and encrypted
Optimum performance	PacketLogic, an optimized passive appliance, sits on the edge of the network and does not impose any requirements on the network infrastructure fabric; therefore it does not impact network performance
Anonymity/transparency of intercept actions	PacketLogic places unobtrusive intercepts for suspect subscribers by implementing very precise extraction rules; the interaction between PLIA, interception, and delivery is automated and encrypted
Flexibility and scalability	PacketLogic platform is modular—additional appliances can be added to manage higher capacity. The Licensing mechanism allows you access to software and hardware upgrades, future proofing your investment, and allowing the BSP to grow to a large provider with only a license change.
Manpower costs	Not substantial since interception and delivery are automated; and the LI function, which can be managed by the Network or System Administrator, is offered through an easy to use software administrative interface (PLIA)
Capital expenditure and operational costs	Only upfront licensing is required with no recurring expenditures. This ensures low per subscriber costs especially as subscriber base grows. In addition, traffic management capabilities allow BSPs to offer value added services to increase revenue, which instantly affect the (OPEX) and investments (CAPEX)
Interruption to BSPs network; increased workload	Receipt of a warrant causes minimal or no disruption in regular operations; neither is the workload increased as interception and delivery are automated, and the LI function, which can be managed by the Network or System Administrator, is offered through an easy to use software administrative interface (PLIA)
Integration	Plug-n-play modular architecture which does not require updates to the network infrastructure ensures seamless integration into the existing network
Network performance	Traffic management capability ensures optimum network performance
Network security	Transparent architecture ensures that packet forwarding interfaces have no identity (IP addresses); they cannot be seen by the users and thus cannot be attacked
Flexibility and scalability	Plug-n-play modular architecture enables selective feature deployment based on license. PacketLogic based networks can grow incrementally by the number of systems, the number of subscribers, as well as by the network bandwidth available for traffic management applications.
New protocols	New and emerging voice and data protocols are constantly added
New services	Provides traffic management capabilities; service providers can offer bandwidth-on-demand, services-on-demand, volume based billing/shaping (VBB/VBS)

Conclusion

The May 14, 2007 CALEA compliance deadline looms large over BSPs. Service providers face tremendous challenges in choosing the right technology, the right solution model with the easiest and least disruptive installation. Technology is critical to ensure compliance and to meet performance, security, and scalability challenges. Secondly, choosing the right implementation model - whether to work with a third party or to completely implement it in-house is a business decision based on pricing, size and growth plans. Technology should not restrict the choice of an implementation model.

PacketLogic is the ideal solution for service providers as it meets CALEA requirements without impacting the performance and security, and can be implemented with no impact on the network switching infrastructure. PacketLogic employs a modular architecture that scales with the BSP's operation and employs Deep Flow Inspection to deliver the most accurate packet classification engine. The PacketLogic platform is extensible and customizable - future proofing the investments in the technology. In addition, the solution is agnostic to the choice of the implementation model - thereby not tying down the BSP in the form of a preferred implementation model.

Finally, PacketLogic offers the best-in-breed policy based traffic management solution which makes your investments deliver a return in the form of efficient bandwidth utilization, and higher revenue realization due to policy based traffic management. All in all, CALEA compliance using PacketLogic technology converts a sunk cost into an investment that pays for itself in the medium term.

Global & US Headquarters
Procera Networks 100 Cooper Court, Los Gatos, CA. 95070
Phone: (408) 354-7200 Fax: (408) 354-7211
Email: info@proceranetworks.com

Sweden/Europe
Procera Networks Hardgatan 13C SE-432 31 Varberg Sweden
Phone: +46-(0)340-48 38 00 Fax: +46-(0)340-48 38 28

Australia / Asia
Procera Networks Pty Ltd Office 206 566 St Kilda Rd Melbourne VIC 3004 Australia
Phone: +61-(0)3-9526 8495 Fax: +61-(0)3-9526 8483

Appendix A: Definitions

Call Identifying Information (CII): dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier. Information includes data such as subscriber's user id, login and logout times, session time, duration, dialed digits and IP address, etc.

Call Content (CC): the entire communication and includes any information concerning the substance or meaning of that communications (audio content of voice call and packets to/from subject)

Collection Function: the location where lawfully authorized intercepted communications (CC and CII) is collected by a LEA.

Interception and Extraction: the function that intercepts and extracts CII and CC from the target suspect's data stream.

Mediation and Delivery: the function that accepts intercepted information from the data interception systems and converts it into a form understandable by LEA (in a specified industry format) and delivering it to them.

Real time: capability that permits a LEA to monitor the target suspect data flow at the time (with minimal latency) it occurs by all parties connected via a conference call when the facilities under surveillance maintain a circuit connection to the call. This includes voice or data flows.

Safe Harbor: a provision stating that service providers are in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or by the FCC.

Subject-initiated dialing and signaling information: capability that permits a LEA to be informed when a target suspect using the facilities under surveillance uses services that provide call identifying information, such as call forwarding, call waiting, call hold, and three-way calling. Excludes signals generated by customer premises equipment when no network signal is generated.

Appendix B: CALEA Implementation Process Comparison

A traditional CALEA compliance solution is compared to Procera Networks' PacketLogic solution. In most solutions, the service provider owns interception by upgrading network elements (routers/switches) and uses a mediation device from another vendor. The edge router, trunking gateway, and the mediation device are key elements in these solutions. For more details, refer to the document *Cisco Service Independent Intercept Architecture Version 1.0.*

The LI administration function sends the intercept provisioning information to the mediation device; while the mediation device sends the intercept information to the collection function. If more than one LEA is intercepting the target for the identical information, the mediation device duplicates the intercept information and sends it to the collection function of each LEA. The illustration explains how the intercept-related information (IRI) and communication content (CC) are sent to the mediation device.

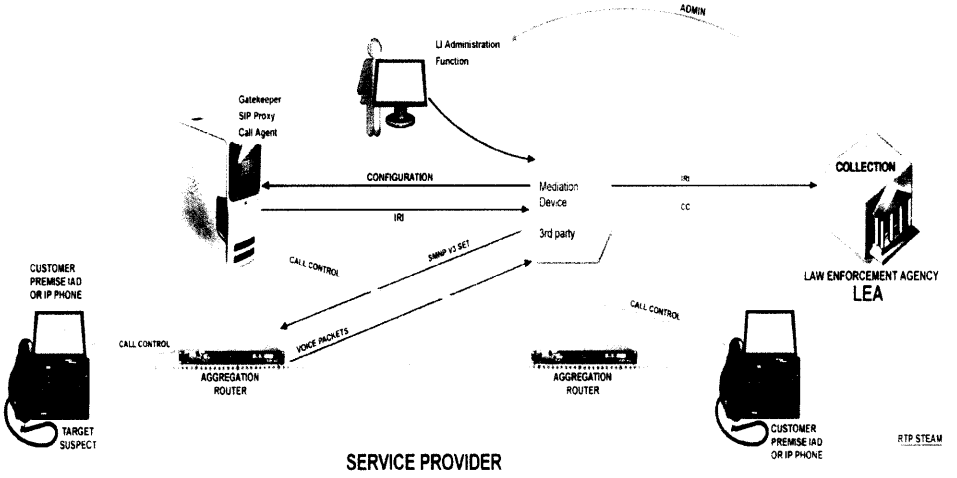


Figure 5: Traditional CALEA Solution

Procera Networks' PacketLogic solution is simple and easy-to-implement. The PacketLogic platform (PLIR) is connected into the service provider's existing network with no infrastructure changes and performs the Interception (PLIR) and Delivery (PLID) process as shown below.

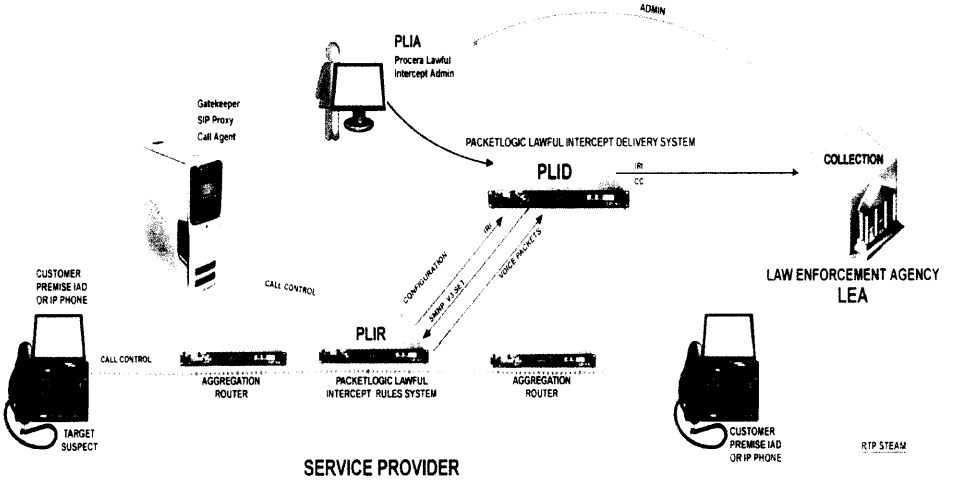


Figure 6: PacketLogic CALEA Solution

Using a traditional CALEA solution, service providers will need to upgrade or add elements in their network infrastructure such as routers, switches, and passive probes in addition to procuring a Mediation device and/or third party services as opposed to using the PacketLogic CALEA solution.

PacketLogic is a passive appliance and seamlessly integrates into the existing network infrastructure. Since it sits on the edge of the network, it functions without imposing any requirements on the network infrastructure fabric—for example, it works without communicating with the gatekeeper.

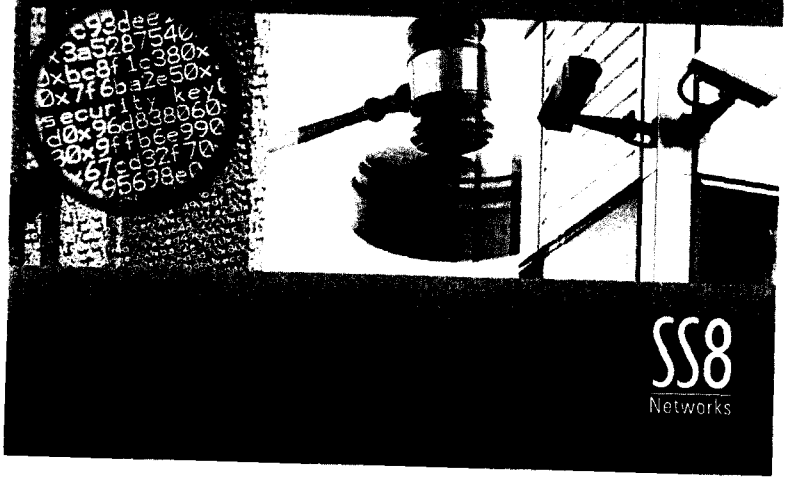
In addition to meeting the CALEA requirements of provisioning Interception and Delivery, PacketLogic provides traffic management capabilities that enable BSPs to grow their business by offering new services to subscribers.

Global & US Headquarters
Procera Networks 100 Cooper Court, Los Gatos, CA. 95070
Phone: (408) 354-7200 Fax: (408) 354-7211
Email: info@proceranetworks.com

Sweden/Europe
Procera Networks Hårdgatan 13C SE-432 31 Varberg Sweden
Phone: +46-(0)340-48 38 00 Fax: +46-(0)340-48 38 28

Australia / Asia
Procera Networks Pty Ltd Office 206 566 St Kilda Rd Melbourne VIC 3004 Australia
Phone: +61-(0)3-9526 8495 Fax: +61-(0)3-9526 8483

THE READY GUIDE TO INTERCEPT LEGISLATION



SS8 Networks

ABOUT THIS GUIDE

Famed author, Henry Miller, once said, "The legal system is often a mystery, and we, its priests, preside over rituals baffling to everyday citizens." In this guide, SS8 has endeavored to identify and summarize this [oft baffling!] legislation, governing lawful intercept within a select number of countries around the world. Information detailing the legislation and polices within these 24 countries is garnered from various open sources and should not be considered conclusive. On the other hand, this guide is free! But should you wish to spend more, we leave the interpretation of these laws to the experts. For as the businessman Franklin P. Jones stated, "Anybody who thinks talk is cheap should get some legal advice."

ABOUT SS8 NETWORKS

Today's electronic surveillance requirements place rigorous yet different demands on carriers and law enforcement agencies. Carriers need to be able to quickly and efficiently identify a target in their network, isolate that target's traffic and get it to law enforcement in a standard, reliable, and legally compliant manner. In turn, law enforcement needs to perform detailed analysis of this information in order to build the story of the target's activities and interactions. Above all, governments need to feel confident that interception capabilities are ahead of the criminal mind. These diverse but intertwined needs are ideally met with an Xcipio-based solution from SS8 Networks.

SS8 Networks is the recognized independent leader in lawful intercept and a worldwide provider of regulatory compliant, electronic surveillance solutions. For nearly fifteen years we have been building networks, futures, cases [for the prosecution] and relationships. Our comprehensive product portfolio covers all three functions of the de facto lawful intercept (LI) architecture: access, mediation and collection. We have deployed proven lawful intercept solutions on all continents, in the networks of the largest wireline, wireless and cable carriers, while also creating non-traditional solutions that include satellite voice carriers, satellite ISPs and WIFI hotspots. Our installations can intercept over 500 million subscribers, and serve over 10,000 law enforcement agents.

SS8 Networks has grown a team with unequalled core competence, a heritage that is undeniable and a solution set that is unparalleled. As the safe choice for carriers, LEAs and governments the world over, SS8 will leave you confident that obligations for national security, criminal prosecution and traffic interception can be fulfilled.

SS8 Networks THE ARCHITECTS OF INTERCEPTS™

TABLE OF CONTENTS

AUSTRALIA

Law Name	Telecommunications (Interception and Access) Act 1979
Related Legislation	1. National Crime Authority Act, 1984 2. Telecommunications Legislation amendment bill, 1997 3. Telecommunications Interception Legislation Amendment Act, 2002 4. The stored communications amendment to the interception act, 2004 5. Telecommunications (interception) amendment bill, 2006
Parties Responsible for Enforcing or Certifying	1. Administrative Appeals Tribunal 2. Attorney General 3. Australian Federal Police 4. Australian Crime Commission 5. Australian Security Intelligence Organization

The first Australian act to legislate interception was the Telephonic Communications Act of 1960. More substantial provisions were made in the Telecommunications (Interception and Access) Act 1979,[1] while other statutes and amendments followed over time. These included the National Crime Authority Act 1984; the Telecommunications Legislation Amendment Bill 1997; the Telecommunications (Interception) Legislation Amendment Act 2000; the Telecommunications Interception Legislation Amendment Act 2002; the Stored Communications Amendment to the Interception Act 2004 and the Telecommunications (Interception) Amendment Bill 2006.

The Telephonic Communications (Interception) Act, 1960 prohibited the interception of communications except under two particular circumstances – threats to national security and drug trafficking. This law was repealed and replaced by the Telecommunications (Interception) Act 1979 (the Interception Act).

The primary objective of the Act of 1979 is to protect the privacy of Australian citizens using any Australian telecommunication channel. However, the exceptions mentioned in paragraph 7(2) (b) continue to authorize the process of legal interception of a communication channel under circumstances of serious offences or national security. Under this act, the law enforcement agencies, such as the Australian Federal Police (AFP) and the Australian Crime Commission (ACC), were for the first time legally allowed to intercept communications. A warrant was required from the law enforcement agencies or the Australian Security Intelligence Organization (ASIO) to authorize this interception.

The Australian Federal Police (AFP) is required to maintain a register of interception instances and submit it to parliament every three months. Section 49 of the Act limits the maximum duration of an issued warrant to 90 days. The Act of 1979 was derived from section 51 of the Australian Constitution Act which gives Parliament the authority to form laws for general peace and order. Amendments made to the bill in 2004 govern interception of stored data.[2]

The first amendment to the act of 1979 was instituted in 1997 and applied to telecom operators, ISPs and carriage service providers (CSPs). The act obligated operators to protect the confidentiality of all communications except when disclosure of relevant information was required and authorised by law.

In 2002, the Telecommunications Interception Legislation Amendment Act was passed. It sought to counter the shortcomings of the previous act and also grant more surveillance powers to the government. It brought into its purview offences involving acts of terrorism, child pornography, etc.[3] On December 8, 2004 the Senate passed the Surveillance Devices Bill, which regulated the use of listening and tracking devices by law enforcement agencies.[4] Prior to that, in November 2004, the Australian Senate passed the 'Stored Communications Amendment to the Inter-

ception Act'. The amendment sought to remove the protection of interception of emails, SMS, and voice mail messages that had not been delivered. By removing the protection, the senate allowed the authorities to intercept the above communications channels without a warrant. The Act however, did not include communication channels such as VoIP.[5] In November 2005, the US Department of Justice expressed the need for the Australian Senate to add coverage of VoIP interception in its legislation.[6] The law was further modified on June 13, 2006 by the Telecommunications (Interception) Amendment Bill 2006 that addressed the content or substance of stored communication (distinct from address of origin and termination) and it obligated law enforcement agencies to provide a 'stored communications warrant' before interception.[7]

The Interception Warrant for National Safety issues can only be issued by the Attorney General. Under special circumstances when the Attorney General (AT) is not in a position to issue the warrant, then it can be issued by the director general of security and approved by the AT. This is unlike law enforcement warrants that can be issued by an eligible judge or a member of the Administrative Appeals Tribunal (AAT).

Warrants issued for the interception of any communication medium, are provided only under the thorough scrutiny of the warrant issuing authorities and only after they have confirmed the extent of the offence and are convinced that all other methods of surveillance have been duly exhausted.

1 Source : http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/
2 Source : http://www.ag.gov.au/
3 Source: http://www.legco.gov.hk/yr04-05/english/sec/library/0405rp02e.pdf
4 Source : http://www.efa.org.au/Issues/Privacy/sd_bill2004.html
5 Source : http://parlinfoweb.aph.gov.au/piweb/Repository/Legis/Bills/Linked/27050402.pdf
6 Source: http://caia.swin.edu.au/talks/CAIA-TALK-060209A.pdf
7 Source: http://www.efa.org.au/Issues/Privacy/ta.html#laws

AUSTRIA

Law Name	Code of Criminal Procedure, 1975
Related Legislation	1. Strafrechtsänderungsgesetz, 2002 2. Überwachungsverordnung, 2001 3. Telecommunications Law 2003
Parties Responsible for Enforcing or Certifying	Court

The Code of Criminal Procedure[8] 1975, also known as Strafprozessordnung (StPO), is the law regulating lawful interception, wiretapping, electronic surveillances, and computer searches in Austria. Other statutes containing provisions for the interception of telecommunications include the amendment BGBl.I 134/2002 (also known as Strafrechtsänderungsgesetz 2002)[9], Überwachungsverordnung[10] (ÜVO), February 2001 and the Telecommunications Law[11] 2003, also known as Telekommunikationsgesetz (TKG 2003). Under UVO, compliance deadlines were set for telecommunication equipment operators (1 June 2001 in accordance with Sections 3 and 4) and network operators (1 January 2005 for compliance with technical handover interface requirements).

Wiretapping provisions are also included in the Code of Criminal Procedure under sections 149a to 149p. Like many statutes that seek to protect privacy, Section 149c (7) of the Code of Criminal Procedure states that the intercepted information needs to be erased in instances where the information has no appropriate use. This Act was further amended on October 1, 2002. The amendment, BGBl. I 134/2002 added new cyber crimes to the list of offences susceptible to lawful intercept and amended some of the prevailing sanctions regarding cyber crime.

In Austria, wiretapping can only be approved, by a judge, for the investigation of criminal cases where the crime is punishable by more than one year in prison. Electronic surveillance, along with

computer access, is authorized for crimes that are punishable by more than 10 years in prison. The stipulations for electronic surveillance and computer access were enforced between 1 October 1997, and 1 July 1998.[12]

In August 2003, the Telecommunications Law 2003 was enacted and obligated telecom operators to provide the necessary surveillance equipment to support lawful interception. According to Section 94 (1) of TKG 2003, telecom operators are required to procure all equipment necessary for the interception of telecom services as stated in the provisions of the Code of Criminal Procedure. Also, according to Section (2) of TKG 2003, the provider has to participate in the interception of the telecom service only to the extent required by law. These obligations apply to all commercial telecom services that broadcast signals over communication networks.

Another ordinance issued in September 2004, by the Federal Minister of Justice, specified that the telecom operators could be compensated on a per-case basis for costs incurred in providing surveillance.[13] The reimbursement included the costs for staff and installation, maintenance, and monitoring of the surveillance equipment.

A draft ordinance, Überwachungsverordnung (ÜVO) was issued in February 2001 by the Federal Minister of Transport, Innovation and Technology, which obligated all telecom operators to install technical equipment for facilitating the surveillance and interception of telecom traffic in compliance with the Code of Criminal Procedure.

According to Section 4 (1) ÜVO, the transmission of the intercepted telecommunication should be performed using standardized transmission paths and protocols. It further specified that carriers must comply with ETSI standard ('201 671 V 1.1.1'[14]), that specifies the handover interface of lawfully intercepted telecom-

munications traffic. Section 4 (2) specifies that for transmission purposes, fixed lines or ISDN dial-up (or similar) connections should be used. In case of dial up connections, the interface should be capable of automatically connecting to the recording device. Also when using a dial-up connection, a connection will be established at the start of each transmission of intercepted telecommunication and released after its completion. According to Section 4 (5), the interception process needs to be kept secret so that neither the suspect nor anyone else knows about it. Moreover, it specifies that the operation of the intercepted subscriber line should not be altered by the surveillance process.

The telecom provider must be capable of providing any intercepted information that is required by the authorities. This includes the address of the subscriber line under surveillance, along with the numbers of all inbound and outbound call attempts, whether they are successful or not. The service provider also needs to track the start time, end time, and the total duration of the call. In the case of mobile phone users, a record of all dialled numbers needs to be maintained. Subject to the court's permission, the authorities can request both the exchange data and the content data from the service provider. The service provider is not only required to assist the authorities in interception but is also obliged to deliver the intercepted information to law enforcement agencies.

8 Source: http://www.internet4jurists.at/gesetze/bg_stpo01.htm
9 Source: http://www.csirt-handbook.org.uk
10 Source: http://www.vibe.at/misc/uevo.en.html
11 Source: http://64.233.179.104/translate_c
12 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005Arg-Chile.pdf
13 Source: http://ris1.bka.gv.at/authentic/findbgbl.aspx?name=entwurf&format=html&docid=COO_2076_100_2_117197
14 Source: http://www.opentap.org/documents/ES201-671.pdf

ARGENTINA

Law Name	The National Intelligence Law No. 25.520, 2001
Related Legislation	1. Information and Intelligence Organic Law 2. Information and Intelligence Control Law 3. Internal Security Law 4. National Defence law 5. Decree No. 950, 2002
Parties Responsible for Enforcing or Certifying	National Directorate for Criminal Intelligence under the jurisdiction of the Minister of Justice, Security and Human Rights

In 1990, Argentina introduced the Information and Intelligence Organic Law; it included a provision for judicial control of interception. Later, in 1993, the Information and Intelligence Control Law was introduced; the bill was a modified version of the Information and Intelligence Organic Law and defined provisions such as technical operations of approved intercepts and penalties for violating the law relating to legal interception. However, in 1995, the United Nations Human Rights Committee expressed its concern over the breadth of the law and this led to the introduction of the National Intelligence Law No. 25.520, which was enacted in November 2001.[15]

Title VI of the National Intelligence Law — Interception and Seizing of Communications — defines provisions for lawful interception and requires operators to have technical capabilities that intercept and forward intercepted communications to the investigating authorities. The law was enhanced in 2002 when a decree was introduced that required telecom operators and ISPs to decrypt their customers' encrypted communications, if the operator was providing the encryption capabilities as part of their service to the customer. It also mandated that operators could not disclose the technical and administrative methods used to comply with their lawful intercept obligations. Such a decree received protests from ISPs and the public; in April 2005, the President

suspended the decree. Currently, the decree is under a process of evaluation for re-introduction.

Under Law 23.984, any investigating authority, requesting an electronic surveillance, needs prior approval from the judiciary;[16] the Secretary of Intelligence is required to file a written request for judicial approval with the Directorate for Judicial Observations or an equivalent judicial authority. Legal requirements for ISPs to build surveillance and wiretapping capabilities are becoming more common with the National Intelligence Law detailing how telecom companies should collaborate with the intelligence agencies to wiretap communications traversing their networks. Further, orders to conduct wiretapping surveillance are only valid for up to 60 days, although the grant can be renewed for another 60 day period. Also, if the government decides not to initiate criminal proceedings against the accused, all evidence collected through the surveillance must be destroyed by the investigating authorities.

There is an exception clause in the bill (under Section 10) which states that the interception warrant is not required in cases of emergency and in circumstances where threats of terrorism or organized crime might pose a danger to property or the lives of individuals. In such cases, communications can be taped without prior judicial order. Intelligence agents are allowed to secretly search, observe, examine, take photographs, record, copy documents, download, or electronically transmit computer media without the need for judicial authorization.[17]

15 Source : http://infoleg.mecon.gov.ar, http://www.dcaf.ch/legal_wg/ev_oslo_030919_estevez.pdf
16 Source : http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-103798
17 Source : http://pi.gn.apc.org/article.shtml?cmd%5B347%5D=x-347-359596&als%5Btheme%5D=Anti%20Terrorism

BELGIUM

Law Name	1. 'wet van 30 juni 1994-ter bescherming van de persoonlijke levenssfeer tegen het afluistereren, kennisnemen en openen van privécommunicatie en telecommunicatie' 2. Loi du 10 juin 1998
Related Legislation	13 Art 259 Code Penal, 30 June 1994
Parties Responsible for Enforcing or Certifying	1. Judicial Police, Investigation Judge, 2. Attorney General, 3. BIPT

The law 'wet van 30 juni 1994-ter bescherming van de persoonlijke levenssfeer tegen het afluistereren, kennisnemen en openen van privécommunicatie en telecommunicatie' regulates lawful interception in Belgium. The provisions include the interception of private conversations and private telecommunications. Prior to the enactment of this law, there was no specific law dealing with lawful interception in Belgium[18].

Surveillance activity conducted under this law can only be executed after a warrant is granted by the investigation judge. Such warrants are granted only in cases where the target is involved in serious crimes such as terrorism. The nominated duration for such surveillance is one month; however, in some circumstances it can be extended by up to six months, after which a new application [for performing surveillance] must be lodged. Unwarranted surveillance activities, such as monitoring, recording, and listening to private communications and private telecommunications (except for the cases described/authorized by the law), are punishable under 13 Art 259 of the Penal Code, 30 June 1994. In cases where the surveillance requires co-operation from telecom operators, the investigation judge must issue orders both to the judicial police and the telecom operator; telecom operators are only required to provide technical assistance during the surveillance. The law also requires that all communications monitored

during the surveillance be recorded and that such recordings be submitted to the investigation judge.

The "wet van..." law was amended in 1997 to remove restrictions on encrypted messages. According to the amendment, the investigation judge could now request experts or network managers to help decrypt intercepted telecom messages; refusal to co-operate for such requests could in turn lead to criminal prosecution.[19] An additional amendment in 1998 mandated greater assistance from telecom operators in performing surveillance and provided more power to the investigation judge and the Attorney General.

According to the law, telecom operators and service providers were also required to record and store calling data and subscribers' identification data for a minimum period of 12 months. In 2003, a new royal decree was enacted to enforce the 'Loi du 10 juin 1998' and provided more details on the practical and technical measures that telecom operators and service providers must comply with to cooperate with law enforcement authorities.

After the adoption of the Interception Law in Belgium in 1994, the number of orders issued for wiretapping increased from 114 in 1996 to 1,000 in 2002, and 1,336 in 2003 to 2,562 in 2004. This increase can be attributed to the increased availability of technical assistance with the creation of the Central Technical Interception Facility (CTIF). In 2005, the number of intercepts per 100,000 inhabitants was 24.4.[20]

18 Source: http://www.cryptome.org/za-esnoop.htm
19 Source: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83525
20 Source: http://www.edri.org/edrigram/number3.12/wiretap

BRAZIL

Law Name	Law 9.296, July 24, 1996
Related Legislation	1. The Telecommunications Act, 1997 2. Code of Criminal
Parties Responsible for Enforcing or Certifying	1. Judge-in-charge 2. Federal police

Law 9.296[21] was introduced in Brazil in 1996. Is purpose was to regulate the constitutional right that protects data and telecommunications privacy. Previously, such surveillance was an ad hoc process without any legal binding.

The new law required the police authority or prosecuting attorney to obtain prior permission from the judge-in-charge for any wiretapping of a suspect. Permission for wiretapping would be granted to the investigating party within 24 hours of filing of the request. Permission to perform a surveillance would only be granted if the suspect was involved in serious crimes, such as corruption, contraband smuggling, murder, kidnapping, or drug smuggling, and there were limited other means to collect evidence against the suspect. Hence, wiretapping is currently only allowed in criminal investigation cases.[22] The law also empowered police authorities to request technical assistance in performing electronic interception

In cases where the interception of telephonic or other electronic communication is undertaken without proper judicial authorization, the individuals involved in such exercise are liable to be prosecuted under Law No 9.296/96.[23]

A wiretap can only be carried out for 15 days, after which the surveillance warrant must be renewed for another 15 days by the judge.[24] After the surveillance is complete, any intercepted communication must be documented for legal usage and complete secrecy must be maintained. In cases where the investigating team is involved in insertion of false data, the members of the

investigating team are liable to be prosecuted, with a prison sentence of up to 12 years, and detention of up to two.

Despite the introduction of law for legal interception, illegal wiretapping by police and intelligence agencies is still common. Examples include the illegal interception of communications involving Itamar Franco, former Vice President of Brazil and illegal communication wiretaps on ministers involved in the Telegate scandal. In addition, a number of inherent weaknesses exist, including resistance on the part of the judges to grant authorization for interception, lack of stringent laws for telecom operators to support such surveillance activities, and insufficient time granted for carrying out such surveillance, which hamper the effectiveness of the law in the country.

21 Source: http://translate.google.com/
22 Source: http://www.oecd.org/dataoecd/12/45/35445196.pdf
23 Source: http://www.informaworld.com/smpp/content~content=a749183160~db=all
24 Source: http://courses.cs.vt.edu/~cs3604/lib/Privacy/International/Group1/GROUP1.HTM

FINLAND

Law Name	Coercive Means Act (Chapter 5a), 1987
Related Legislation	1. Act on the Protection of Privacy in Electronic Communications, 2004 2. Act 1995/402 3. Police Act, 2001
Parties Responsible for Enforcing or Certifying	1. Court 2. The Finnish Communications Regulatory Authority

Lawful interception in Finland is governed by the Coercive Means Act (Chapter 5a), as amended by the Act 1995/402. This Act includes provisions for the metering of telecommunications, bugging of telecommunications, and technical surveillance.[25] Telecommunication interception includes the interception of fixed-line telephones, mobile phones, and e-mails.

Authorization for performing interception is obtained through a court of law. The application for authorization has to be made in writing by the police or by an official who has the authority to arrest.[26] The wiretapping is only authorized if the intercepted information is considered to be of utmost importance to the case proceedings. Wiretapping is permitted in the investigation of serious crimes, such as skyjacking, narcotics offences, treason, etc. While interception warrants are valid for no more than one month, depending upon the severity of the situation, the police can file a new application for extension.

Metering of telecommunications (i.e acquiring intercept related information/call signalling) is authorized in investigations of computer crimes, drug-related crimes, or cases in which prosecution can lead to sentencing of at least four months in prison. However, telecommunications 'bugging' (interception of actual call content) is only granted for suspects accused of drug peddling or for any other crime in which the punishment is at least four years imprisonment.

Section 3 of the Police Act, 2001[27] authorizes the police to use technical surveillance and metering of telecommunications for reconnaissance purposes. Also, the Act on the Protection of Privacy in Electronic Communications,[28] which was enforced on September 1, 2004, expanded the scope for police access to telecommunication information in the investigation of criminal cases. The Act of 2004 replaced the Protection of Privacy and Data Security Act of 2000. It also expanded the definitions of telecommunications to include e-mails and all Internet-based communications. In all cases, the police are authorized to acquire a dynamic IP address and the international mobile equipment identity (IMEI) numbers of mobile phones. The Finnish Communications Regulatory Authority (FICORA) enforces these acts and ensures compliance.[29]

The number of intercepted cases in Finland is far fewer than in other European countries.

25 Source: http://www-rohan.sdsu.edu/faculty/rwinslow/europe/finland.html
26 Source: http://www.coe.int/t/dg1/Greco/evaluations/round2/GrecoEval2(2003)3_Finland_EN.pdf
27 Source: http://www.finlex.fi/en/laki/kaannokset/1995/en19950493.pdf
28 Source: http://www.finlex.fi/en/laki/kaannokset/2004/en20040516.pdf
29 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005china-georgia.pdf

FRANCE

Law Name	1. Code of Criminal Proceedings 2. Telecommunications Correspondence (Secrecy) Act, 1991
Related Legislation	1. Fiscal Procedure Code 2. Monetary and Financial Code 3. Data Protection Act 4. Posts and Telecommunications Code 5. Freedom of Communication Act 6. Decree No. 93-119 7. Decree No. 2002-997 8. Law for Interior Safety 9. Everyday Security Act
Parties Responsible for Enforcing or Certifying	1. Court 2. Ministry of Interior

There are many French laws regulating the lawful interception of telecommunications. The predominant legislation is the Telecommunications Correspondence (Secrecy) Act[30] (Loi sur le secret des correspondances, Law No. 91-646), July 10, 1991, otherwise referred to as the "1991 Act." Other statutes have also made provisions for lawfully intercepting communications: the Code of Criminal Procedure;[31] the Fiscal Procedure Code; the Monetary and Financial Code; the Data Protection Act[32] (Loi informatique et libertés, Law No. 78-17), January 6, 1978; the Posts and Telecommunications Code; the Freedom of Communication Act'[33] (Loi relative à la liberté de communication, Law No. 86-1067), September 30, 1986, as amended by the Law of August 1, 2000, the Decree No. 93-119, January 28, 1993; the Decree No. 2002-997[34], July 16, 2002; the Law for Interior Safety (Loi de Sécurité Intérieure, Law No. 2003-239) March 18, 2003; and the Everyday Security Act[35] (Loi sur la Sécurité Quotidienne or LSQ, Law No.2001-1062), November 15, 2001.[36]

Article 1 of the 1991 Act authorises the lawful interception of telecommunications. Telecommunication service providers are obligated to intercept communications when authorized under Articles 100 to 100–7 of the Code of Criminal Procedure, by an investigating judge, the Courts of Assize or by the French Supreme Court of Appeal (Cour de Cassation). The service providers are also required to intercept telecommunications in cases where authorization is granted by the Prime Minister. These interceptions are permitted for the prevention of serious offences, such as terrorism, espionage, or threat to national security. According to Article 11–1 of the 1991 Act, the telecommunication service provider is obligated to provide a decrypted version of encrypted information or alternatively to give the decryption keys to the authorities.

A warrant for interception is issued in writing and must contain the number of the intercepted subscriber and the duration of interception. Warrants are valid for a maximum period of four months but can be renewed under Article 6 of the 1991 Act. Article 9 of the 1991 Act mandates that law enforcement authorities destroy intercepted information, under the supervision of the Prime Minister, within 10 days of interception.

According to Article L.35-5 of the Postal and Telecommunications Code, service providers must provide access to all information required by the authorities. This information may include the most updated list of subscribers and users, their addresses and any numbers dialed.

Article D.98-1 of the Postal and Telecommunications Code compels service providers to work with LEAs in conducting electronic surveillance; operators are supposed to install and make available the technical equipment required for interception. Article D.99 states that any independent network operator shall

also comply with the LEAs in situations related to public safety or defence. Data can be retained by telecommunication service operators for a maximum of one year under the provision of Article L32-3-1 of the Postal and Telecommunications Code.

The costs for deploying intercept technology, and the subsequent maintenance thereof, are covered by the French government under Article 35-6 of the Postal and Telecommunications Code. Operating costs for performing interception and the cost of connections for transmission of intercepted information are also reimbursed by the government.

Other statutes with wiretapping provisions include 1) the Everyday Security Act (Article 22), which provides for the use of new technologies in the field of communication and information to prevent serious crimes, such as terrorism, narcotics, etc, 2) Decree No. 93-119, issued to appoint officials to supervise installations of the equipment necessary for providing interception in accordance with the 1991 Act, 3) Decree No. 2002-997, which covered telecommunication service providers carrying encrypted traffic, 4) The Law for Interior Safety, which prescribed the powers given to state and local authorities for the protection of people and goods, 5) The Data Protection Act, which covers the access to data and files, and 6) The Monetary and Financial Code, which grants powers to investigators to summon telecom operators to provide them with certain information.

For national oversight, the Commission nationale de contrôle des interceptions de sécurité (CNCIS) was created to lay down rules and regulations regarding interception of communication. CNCIS also has the responsibility for reviewing the number of wiretapping cases every year. The number of authorized interceptions of telecommunications from 1995 to 1999 was between

4,500 and 4,700.[37] There were 5,651 authorized interceptions in 2004. Of these, 3,733 were initial interceptions and 1,918 were renewals.[38] During 2005 and 2006, there were 5,774 (4,067 initial interceptions and 1,707 renewals) and 5,985 (4,176 initial interceptions and 1,809 renewals) official interceptions, respectively.[39]

30 Source: http://www.legifrance.gouv.fr/texteconsolide/PCEAR.htm
31 Source: http://195.83.177.9/upl/pdf/code_34.pdf
32 Source: http://195.83.177.9/code/liste.phtml?lang=uk&c=25&r=1061, http://www.legifrance.gouv.fr/texteconsolide
33 Source: http://www.legifrance.gouv.fr/html/codes_traduits, http://www.legifrance.gouv.fr/texteconsolide
34 Source: http://www.legifrance.gouv.fr/texteconsolide, http://www.legifrance.gouv.fr/texteconsolide
35 Source: http://www.legifrance.gouv.fr/texteconsolide, http://www.legifrance.gouv.fr/texteconsolide
36 Source: http://www.minez.nl
37 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005china-georgia.pdf
38 Source: http://www.ladocumentationfrancaise.fr/informations/presse/2005/interceptions-securite.shtml
39 Source: http://lesrapports.ladocumentationfrancaise.fr/BRP/074000237/0000.pdf

GERMANY

Law Name	1. Telecommunications Act, 2004 2. Telecommunications Interception Ordinance, 2002 3. The Act on the Restriction of the Privacy of Correspondence, Posts, and Telecommunications, 2001 4. Telecommunications Act, 1996 5. Criminal Procedure Code, 1987
Related Legislation	1. Foreign Trade and Payments Act, 1961 2. Customs Investigation Service Act
Parties Responsible for Enforcing or Certifying	1. Judge 2. Ministry of Interior

In Germany, lawful interception of communications through wiretapping and recording of IP-based network communication is approved by a number of statutes. The main laws governing the interception of telecommunications are the Criminal Procedure Code[40] (Strafprozeßordnung, StPO), April 7, 1987; the Telecommunications Act[41] (TKG), July 25, 1996; the Act on the Restriction of the Privacy of Correspondence, Posts, and Telecommunications (G-10), June 26, 2001; the Telecommunications Monitoring Regulation[42] (TKÜV), January 22, 2002 and the Telecommunications Act[43] (TKG), June 22, 2004. Other laws having provisions for wiretapping are the Foreign Trade and Payments Act (AWG), April 20, 1961, and the Customs Investigation Service Act (ZFdG).[44]

Interception can be carried out in criminal cases, such as homicide, narcotics, etc., or in cases of threat to the national security of Germany. Under Section 100a of the Criminal Procedure Code, such interceptions must be authorized by a judge. This authorization is given in writing and can remain enforced for a period of three to six months, according to Section 100b (2) of the Criminal Procedure Code. The German Minister of Interior can also order the interception of telecommunications. In cases of extreme urgency, the public prosecutor may authorize the interception.

The G-10 Act authorizes federal and state law enforcement agencies to intercept and record telecommunications and to open and scrutinize postal packets. The AWG authorizes the Customs Criminological Office to intercept and record telecommunications. Further details are included in Section 100(a) of the Criminal Procedure Code.

According to the definitions of 'telecommunications' and 'telecommunications systems' given in Section 3(16) and Section 3(17) of the TKG 1996, telecommunications covers all aspects of IP communications including VoIP, Web hosting, e-mail, and Internet services.

The German interception laws also impose obligations on telecom operators. Section 88 of the TKG 1996 states that the telecommunication service operator needs to configure and keep available technical facilities for implementing interception of telecommunications. According to Section 88 (2) of the TKG 1996, telecom operator systems are only permitted to operate when these interception facilities are approved by the Regulatory Authority for Telecommunication and Mail (Regulierungsbehörde für Telekommunikation und Post; RegTP). Section 2 of the G-10 law and Section 88 (4) of the TKG 1996 then clearly states that operators will use these capabilities to intercept call signaling and content. Operators are also compelled to hand over any e-mails transmitted over their networks, and to provide ready network access for transferring the intercepted information.

On June 22, 2004, the German Parliament adopted the Telecommunications Act complying with the European Parliament's decision to modify the existing telecommunications law in May 2002. Part 7 of this TKG 2004 includes all the provisions for privacy of telecommunications, data protection, and public safety. This Act, under Section 110, also requires telecom operators to deploy the technical facilities necessary for implementing interception at their own expense.[45]

The TKÜV regulates the technical and organizational requirements for interception of telecommunications. This ordinance was amended in August 2002. Section 21 of the TKÜV provides for potential relaxation toward telecommunication operators with less than 10,000 subscribers; in section 3 (2)(5), TKÜV states that the obligations for service providers with less than 1,000 subscribers is limited to assisting authorities with intercepting and recording calls. All telecommunication companies need to align themselves to the stipulated technical standards in compliance with the legal obligations under TKÜV. These standards have been specified in the Technical Directive of TR TKÜ 3.1,[46] issued by the RegTP in May 2002. This directive was a joint effort of the service providers, law enforcement agencies, telecommunications equipment manufacturers, and regulatory authorities. January 1, 2005 was the stipulated deadline given by the TKÜV for providers to either procure new equipment or modify the existing equipment for interception with respect to the ordinance's directive.

There has been a quantum leap of nearly 500 percent in the number of wiretapping cases in Germany within a decade. In 1994, there were 4,674 cases of monitoring. By comparison, there were 29,017 cases of lawful interception in 2004.[47]

40 Source: http://www.iuscomp.org/gla/statutes/StPO.htm#100
41 Source: http://www.iuscomp.org/gla/statutes/TKG.htm
42 Source: http://217.160.60.235/BGBL/bgbl1f/bgbl102005s458.pdf
43 Source: http://www.bfdi.bund.de/cln_030/nn_946430/EN
44 Source: http://www.minez.nl/, http://cyber.law.harvard.edu/globaleconomy, http://www.datenschutz-berlin.de
45 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005china-georgia.pdf
46 Source: http://www.eco.de/servlet/PB/show/1223643/20030515-TR-TKUE-EN.pdf
47 Source: http://www.heise.de/newsticker/meldung/58104

INDIA

Law Name	1. The Indian Telegraph Act, 1885 2. The Information Technology Act, 2000
Related Legislation	1. Indian Wireless Telegraphy Act, 1933 2. The Unlawful Activities Prevention Act, 1967 3. The Information Technology (Amendment) Bill, 2006 (Proposed) 4. Prevention of Terrorist Activities Act, 2002 (POTA)
Parties Responsible for Enforcing or Certifying	Union Home Secretary

In India, various laws have been passed to govern lawful interception. The Indian Telegraph Act, 1885 laid the country's foundation for lawful interception of communications. Subsequently, the Act was modified as the Indian Wireless Telegraphy Act, 1933. Other laws that followed were the Unlawful Activities Prevention Act, 1967, and the Information Technology Act, 2000. An amendment to the latter was proposed in 2006 and is known as the Information Technology (Amendment) Bill, 2006.

According to the Indian Telegraph Act, 1885, the word telegraph extended to all devices and instruments that could be used for the purpose of transmission of messages. It gave powers to the Indian government to intercept any form of telegraph during national emergency;[48] although it could only be done with the authorization of the central or state government. The Act was later modified in 1933 under the name of the Indian Wireless Telegraphy Act and was extended to wireless telegraphy equipment. The act also prohibited the general public from possessing a wireless transmission apparatus without a licence.[49] In 1967, the government passed the Unlawful Activities Prevention Act, which authorized police forces to use information obtained through interception of communication channels as evidence in trials.

The Telegraph Act, 1885, was further amended in 1996 by the Supreme Court, which ruled that wiretapping amounted to invasion of privacy, and was therefore a serious legal offence, unless conducted under appropriate guidelines. In the interest of national security and the issues related to law and order, the Supreme Court thus laid out clear guidelines for wiretapping, granting power of authorization to the Union Home Secretary in central government or his counterparts at the state level.

The Information Technology Act, the main act governing the interception of communication in cyber space, was passed by the Indian government in May 2000. Section 69 of the Act authorized law enforcement agencies to intercept any form of communication transmitted via a computer. Discretion for authorization in turn lies with the Controller of Certifying Authorities (CCA).[50]

In 2002, the Indian Parliament passed the Prevention of Terrorism Activities Act (POTA) that gave sweeping powers to law enforcement agencies to conduct interception of all communication channels being used for terrorist acts.

In 2001, a communications convergence bill was proposed in the Indian Parliament; it has not been passed by the house to date. If passed, it will give powers to the government or any officer to intercept a communication channel if required to do so in the interest of national safety or maintaining harmony with neighboring countries. It will also outline the penalties and punishments of telecom operators in the event of non-cooperation with law enforcement authorities.[51]

A proposal has also been made in Parliament for amendment of the Information Technology Act of 2000, known as the Information Technology (Amendment) Bill, 2006. It proposes to confirm the powers of the government to intercept and monitor any communication channel in the face of threats to national integrity and sovereignty and to oblige operators to aid law enforcement

agencies by providing them with access to computer resources and assistance in intercepting, monitoring, and decrypting any data suspected to be of critical nature — failing which, they would be punishable by law.[52]

48 Source : http://www.dot.gov.in/Acts/telegraphact.htm
49 Source : http://www.dot.gov.in/Acts/wirelessact.htm
50 Source : http://www.privacyinternational.org/survey/phr2003/countries/india.htm
51 Source : http://www.dot.gov.in/Acts/draftconvergence.pdf
52 Source : http://164.100.24.208/ls/bills-ls-rs/2006/96_2006.pdf

IRELAND

Law Name	Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993
Related Legislation	1. Postal and Telecommunications Services Act, 1983 2. Post Office (Amendment) Act, 1951 3. Official Secrets Act, 1963 4. The Criminal Justice (Terrorist Offences) Act, 2005
Parties Responsible for Enforcing or Certifying	1. Minister for Justice 2. Commissioner of the Garda Síochána

Passed as an amendment to the Postal and Telecommunications Services Act, 1983, the 'Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993'[53] is Ireland's legislation to govern lawful 'phone-tapping', 'wiretapping' and electronic surveillance.

This Act defines 'interception' and the process for legally intercepting both postal packets and telecommunications messages. For authorization, a written application must be sent to either the Commissioner of the Garda Síochána (Commissioner) or the Minister for Justice (Minister). This authorization is granted by the Minister or the Commissioner in cases of a threat to state security. In cases of exceptional urgency, this authorization can be given orally by the Minister, but needs to be substantiated into a warrant at the earliest opportunity. For cases pertaining to criminal investigations, the authorization is granted only by the Commissioner in the form of a warrant.

The warrant should include the date on which authorization is granted and the postal addresses of concerned parties, the type of proposed interception (postal packets, telecommunications messages or both), and the need for disclosure of intercepted materials. Under Sections 7 and 8 (6) of the Act, the warrant

remains in force for a period of not more than six months, but can be extended under the provisions provided in Subsection (6). Under Section 11 (1) of the Act, all official documents related to application and authorization must be retained for a minimum of three years from the date on which the warrant expires.

Section 110 of the Act makes it mandatory for telecom service providers to also retain data for 36 months. Similarly, the Criminal Justice (Terrorist Offences) Act 2005 states that all official documents including authorization and its application should be retained for at least three years at all fixed-line and mobile phone service providers from the date on which the authorization is enforced.[54]

The Freedom of Information Act, 1997[55] (FOI Act, 1997) enables the public to access the information held by government agecies. The information can include the intercepted telephone records of individuals. However, Section 32(1) (b) of the Act[56] grants permission to the government agencies to refuse an individual's request for disclosure of information regarding his/her intercepted telephone records. This is also in compliance with Section 12 of Act of 1993, which permits the non-disclosure of certain intercepted records of individuals.

The concept of interception of communications was embedded in the Postal and Telecommunications Services Act, 1983[57], Section 98, which prohibited the interception of telecommunication messages. It authorized members of the Garda Síochána to intercept telecommunication messages for a complaint received regarding suspected offences under Section 13 of the Post Office (Amendment) Act, 1951.[58] Such an interception could also be carried out after obtaining permission from the Minister under Section 110, of the Act of 1983.

53 Source: http://www.irishstatutebook.ie/ZZA10Y1993.html
54 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005greece-latvia.pdf
55 Source: http://www.finance.gov.ie/viewdoc.asp?DocID=837
56 Source: http://www.oic.gov.ie/en/DecisionsoftheCommissioner/LetterDecisions/Name,1037,en.htm
57 Source : http://www.irishstatutebook.ie/1983/en/act/pub/0024/index.html
58 Source: http://www.irishstatutebook.ie/ZZA17Y1951.html

ISRAEL

Law Name	The Secret Monitoring Law, 1979 Related Legislation The Computer Law, 1995
Related Legislation	The Computer Law, 1995
Parties Responsible for Enforcing or Certifying	1. President of the District Court 2. Chief Military Censor

The Secret Monitoring Law, passed in 1979, serves as Israel's primary interception legislation. This law permits the legal use of wiretapping and other means for intercepting communications.[59]

Under this law, Israeli police require permission from the President of the District Court before intercepting any form of wire or electronic communication. The law also permits the use of a microphone for interception. Warrants are issued for three months and can be renewed if required. The Chief Military Censor can also intercept cross-border or international calls to or from Israel for censorship purposes. In addition, intelligence agencies may wiretap suspects who potentially jeopardize national security, but only after receiving written permission from either the Prime Minister or Defence Minister.

The Secret Monitoring Law was amended in 1995 in view of findings filed by the State Comptroller, highlighting the abuse of wiretapping procedures by the police force; procedures were tightened accordingly. In addition, the amendment also widened the scope of the Act to cover new technologies such as mobile and Internet/PC communication, including e-mails. The collection of e-mail would be legal for targets who have been accused of a crime, but who have not been convicted to date. This modification in the law also increased the penalties for illegal wiretapping and permitted the interception of privileged communications, such as conversations with doctors, lawyers, etc. In turn, law enforce-

ment agencies must present an annual report that details all interception activities, to the Knesset (Israeli Parliament).

The Postal and Telegraph Censor, the civil department under the Ministry of Defence, has the authority to scrutinize any postal mail or courier in order to maintain civil order or national security. The Computer Law 1995 prohibits and penalizes unauthorized access to a computer.

According to official records, the number of wiretapping cases carried out by the police in 1999, 2000, and 2002 was 1,700, 1,685 and 1,089, respectively. The 2005 annual report by the police suggested that out of 1,095 requests by police for wiretapping, 1,089 were approved by the district court.[60]

59 Source: http://www.privacyinternational.org/survey/phr2003/countries/israel.htm
60 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005greece-latvia.pdf

ITALY

Law Name	Penal Procedure Code (Articles 266–271)
Related Legislation	1. Computer Crime Law, 1993 2. Act No.140 (2003) 3. Act No.45 (2004)
Parties Responsible for Enforcing or Certifying	1. Garante 2. Court

In Italy, lawful wiretapping is regulated by Articles 266 to 271 of the Penal Procedure Code.[61] This authorization is provided in cases pertaining to legal proceedings. These articles also include the types of communications which can be lawfully intercepted.

Prior to the interception of communication, a court approval is required. This approval lasts for 15 days, but can be renewed for a further 15 days if required. Intercept data (excluding location data) must also be retained for a period of 4 years, (increased from 30 months in February 2004 by Act No. 45/2004). The increased data retention period applies only to telephony traffic data. Location data on fixed line and mobile telephony must be retained for 29 months. Operators must also retain the records of all unsuccessful dial attempts. In addition, ISPs need to retain all data for at least six months.[62]

Judges monitor the procedures for recording and storing intercepted information. Any information which is not used is destroyed. However, conversations of religious ministers, doctors, lawyers, and other professionals that are categorized under professional confidentiality rules cannot be intercepted. Conversely, there are more lenient procedures for Anti-mafia cases when issuing a warrant for the interception of communications. In October 2001, the government reached a verdict on facilitating telephone tapping and electronic surveillance when considering serious offences, such as drug peddling, murder, etc. This practice only required the authorization and supervision of judicial authorities.

A report submitted in June 2002 indicated that Rome witnessed around 13,000 cases of legal wiretaps over a period of one year. According to some sources*, Italy is the world's most wiretapped country. In 1992, around 15,000 cases were authorized, and this had increased to 44,000 by1996. The exponential increase in the number of legalized interceptions continued into the 21st century: In 2002, 2003, and 2004, the numbers of interception cases stood at 45,000, 77,000, and 100,000[63], respectively. The wiretapping cases increased three-fold from 32,000 in 2001 to 106,000 in 2005.[64]

*Based on 2002 statistics – 76 wiretaps per 100,000 inhabitants.[65] The main reason for this high level of wiretapping could be traced to an Italian law of 1992. This law allows wiretapping to be implemented on a per crime basis by order of a prosecutor, and does not require prior approval or supervision from judicial authorities. That said, the intercepted information cannot be used as evidence but can assist in the preparation of cases.

61 Source: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83522
62 Source: http://en.wikipedia.org/wiki/Data_retention
63 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005greece-latvia.pdf
64 Source: http://www.akdart.com/priv7.html
65 Source: http://www.edri.org/edrigram/number2.21/wiretaps

JAPAN

Law Name	Communications Interception Law, 1999
Related Legislation	None
Parties Responsible for Enforcing or Certifying	Court

The Communications Interception Law, 1999, governs lawful interception in Japan. Prior to the enforcement of this law, wiretapping was prohibited and considered illegal under Article 14 of Japan's Wire Telecommunications Law and Article 104 of Japan's Telecommunications Business Law, and a violation of the Constitutional Right of Privacy.[66]

The Communications Interception Law was passed by the Japanese legislative assembly (Diet) in August 1999, but it was enacted in August 2000 after several amendments. The law permits the law enforcement agencies (LEAs) to intercept communications on phone, fax, and the Internet in criminal cases involving organized murder, illicit firearms trade, drug trafficking, and smuggling of illegal immigrants into Japan. However, the communications of doctors, lawyers, and religious leaders cannot be intercepted under the law[67] and media communications can only be intercepted under certain conditions.[68] The law also directs ISPs to maintain a log of all the Internet communications that are monitored at any time.

According to the law, LEAs, which include prosecutors, police officers at the rank of superintendent and above, narcotic controllers, and Japan's Maritime Safety Agency officials, can execute wiretapping upon receipt of an authorized warrant. The warrants are issued by the district court judges for 10 days and can be extended up to thirty. The law also requires the presence of a third-party non-police witness, such as an employee of either the communication service provider or regional government, for monitoring the wiretapping process. In addition, LEAs are required to

notify individuals (whose communications have been intercepted) within 30 days of concluding the investigation and all documents pertaining to the communication must be destroyed thereafter.[69] To prevent the abuse of the law, spot monitoring (only some portions of communications can be intercepted and the process must terminate if the communication is considered to be innocent) is used for wiretapping. And in cases involving investigations by prosecutors, the court warrant is issued by a chief prosecutor, the head of the regional prosecutor's office.

The law does not define the devices or surveillance tools that can be used for lawful interception.[70] According to officials in the Ministry of Justice, only five authorized wiretaps were conducted in 2005, but the number is expected to increase considerably in the future.[71]

66 Source: http://www.csd.uwo.ca/~markp/htmls/Echelon2.pdf
67 Source: http://www.csd.uwo.ca/~markp/htmls/Echelon2.pdf
68 Source: http://www.snapshield.com/www_problems/Japan/Wiretap_but_carefully.htm
69 Source: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83523#_ftn22
70 Source: http://www.glo.org/?q=node/976
71 Source: http://search.japantimes.co.jp/cgi-bin/nn20070217a9.html

REPUBLIC OF KOREA

Law Name	Protection of Communications Secrets Act 1993
Related Legislation	None
Parties Responsible for Enforcing or Certifying	1. Police 2. High Court Judge

The Protection of Communications Secrets Act[72] 1993, also known as the Anti-Wiretap Law, regulates lawful interception in the Republic of Korea. This Act defines situations in which the government may intercept communications through telephone calls, post, mail, or other forms of communication. The intercepted information can be used as evidence in civil court or criminal cases.

According to this act, a government official — such as the prosecutor — needs to seek prior permission from a court for authorization to intercept communications. These applications for interception should be in writing and approved surveillances are usually conducted for two months in the case of criminal investigation. For issues relating to national security, the head of intelligence and investigative agencies must secure a warrant from the Senior Chief Judge of the High Court or an approval from the President. In these cases, surveillance periods of up to four months[73] may be granted. In all cases, applications for warrants should specify the reason for interception.

In November 1999, the Korean government proposed to amend the Protection of Communications Secrets Act (1993), which would allow victims of illegal wiretapping to bring charges against the government and thus curb the number of unauthorized wiretapping cases. In turn, the government established a 'wiretapping complaint center' under the Ministry of Information and Communication (MIC) in 1999.

On November 9, 2004, a proposal was submitted by the government to the Korean National Assembly to amend the law regulating the privacy of communications. This proposed bill aimed to make it mandatory for investigating authorities to obtain an approval from a district court judge prior to tracking the location of a mobile phone user. In addition, the user must be made aware of this tracking within three months of providing the information to the governing authorities.[74]

There were 2,884 wiretapping cases reported in Korea in 2001, reflecting a 21 percent increase from the year 2000.[75] The government departments had made a total of 270,584 requests (both call signalling and call content) for interception of telecommunication in 2001, reflecting a 66.8 percent increase over 2000. MIC carried out 528 wiretapping requests from January to June in 2006 compared to 550 cases in the same period in 2005.[76]

72 Source: www.ictparliament.org/CDTunisi/ict_compendium/paesi/corea/COR27.pdf
73 Source: http://www.state.gov/g/drl/rls/hrrpt/2006/78778.htm
74 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005peru-srl.pdf
75 Source: http://www.privacy.org/pi/issues/tapping/
76 Source: http://www.state.gov/g/drl/rls/hrrpt/2006/78778.htm

THE NETHERLANDS

Law Name	1. Code of Criminal Proceedings 2. Telecommunications Act, 1998
Related Legislation	1. The Special Investigation Powers Act, 2000 2. Intelligence and Security Services Act, 2002 3. Vorderen gegevens telecommunicatie, 2004 4. Functional Specification for lawful interception of Internet traffic in the Netherlands 5. Transport of Intercepted IP Traffic
Parties Responsible for Enforcing or Certifying	1. Court 2. Ministry of Interior 3. Minister of Economic Affairs 4. Minister of Justice

In the Netherlands, there are a number of laws governing the lawful interception of telecommunications including the Code of Criminal Proceedings (Wetboek van Strafvordering), Telecommunications Act (Telecommunicatiewet or TW) October 19, 1998, The Special Investigation Powers Act[77] or 'Wet BOB' (Wet Bijzondere OpsporingsBevoegdheden) February 1, 2000, and the Intelligence and Security Services Act[78] (Wet Inlichtingen en Veiligheidsdiensten), February 7, 2002.[79]

In addition to wiretapping, the interception of telecommunications extends to publicly available Internet services such as e-mails, chat, and web surfing. A warrant authorization is required before wiretapping or interception procedures can commence. The interception of communications for investigation of criminal cases is authorized by a court and is granted under Article 125m of the Code of Criminal Proceedings.[80] Specifically, Articles 126m and 126t authorize content interception, while Articles 126n and 126u authorize traffic data interception. In contrast, intercept activities conducted by intelligence agencies are authorized by the Minister of Interior.

The Telecommunications Act (TW) lists specific obligations for telecommunication service and access providers. Under Article 13.1 Paragraph 1, telecommunication service providers can only offer commercial services if the associated networks are wiretap-enabled. Service providers are then obligated to assist LEAs in the lawful interception of communications under Article 13.2. Article 13.4 Paragraph 1 mandates that service providers share all the information (subscriber's number, address, city, type of service, etc.) required by LEAs for carrying out interception orders. In addition, the operators must store traffic data for at least three months for data analysis. Article 13.8 offers provisions under 'special circumstances' which permits an exemption from the wiretapping obligations. This exemption can be granted only by the Minister of Economic Affairs in consultation with the Minister of the Interior and the Minister of Justice. However, the 'special circumstances' are somewhat ambiguous as they do not define the circumstances which fall under this category.[81]

Under TW Article 13.6, telecommunication service providers must bear the installation, maintenance, and overhead costs for enabling network wiretap capabilities, while the government reimburses only the administrative and labor costs for transferring intercepted traffic to LEAs. A recent law, 'Vorderen gegevens telecommunicatie' enforced in September 2004, also authorizes the public prosecutor to request traffic data from telecommunication service providers, although this authorization may only be granted if conviction on the crime would result in punishment of at least four years imprisonment.

The Intelligence and Security Services Act authorizes LEAs to intercept, search and scan satellite communications. It also permits the intelligence agencies to retain the intercepted information for a maximum period of one year.

The Special Investigation Powers Act was incorporated in order to streamline investigation methods for criminal cases.

There are also two specifications for the lawful interception of Internet communications — Functional Specification for lawful interception of Internet traffic in the Netherlands,[82] or the WAI Functional Specification — and the Transport of Intercepted IP Traffic[83] (TIIT). The WAI Functional Specification applies specifically to IP and email interception, while TIIT provides details on the handover interfaces (to law enforcement).

According to a 2003 report by the German Max Planck Institute for Foreign and International Criminal Law, the Netherlands is the world's second-most wiretapped nation. The Netherlands has an average of 62 wiretaps per 100,000 inhabitants, after Italy with 76 wiretaps.[84]

77 Source: http://english.justitie.nl/images/Special%20powers%20of%20investigation%20act_tcm35-14199.pdf
78 Source: http://www.eerstekamer.nl/9324000/1/j9vvgh5ihkk7kof/vg4nel1rvb0h/f=x.pdf
79 Source: http://wwwes.cs.utwente.nl/safe-nl/meetings/29-11-2002/lawful-intercept.pdf
80 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005lith-peru.pdf
81 Source: http://www.minez.nl/
82 Source: http://cryptome.org/nl-tap-specs.htm
83 Source: http://www.opentap.org/documents/TIiT-v0.1.2.pdf
84 Source: http://www.edri.org/edrigram/number2.21/wiretaps

NEW ZEALAND

Law Name	1. Telecommunications (Interception Capability) Act 2004 2. Government Communications Security Bureau Act 2003 3. International Terrorism (Emergency Powers) Act 1987 4. Misuse of Drugs Amendment Act 1978 5. New Zealand Security Intelligence Service Act 1969 6. Crimes Act 1961
Related Legislation	1. Crimes Amendment Act 2003 2. New Zealand Security Intelligence Service *Amendment* Act 1999 3. New Zealand Security Intelligence Service Amendment (No. 2) Act 1999
Parties Responsible for Enforcing or Certifying	1. Judge of a High Court 2. The Minister in charge of New Zealand Security Intelligence Service (NZSIS) 3. The Commissioner of Security Warrants

In New Zealand, the interception of telecommunication is governed by many laws including the Telecommunications (Interception Capability) Act 2004, Government Communications Security Bureau Act 2003, International Terrorism (Emergency Powers) Act 1987, Misuse of Drugs Amendment Act 1978, New Zealand Security Intelligence Service Act 1969, and Crimes Act 1961.

The Crimes Act 1961, Misuse of Drugs Amendment Act 1978, and International Terrorism (Emergency Powers) Act 1987 gave powers to the New Zealand police to intercept private communications under specific provisions; under the Crimes Act[85] the New Zealand police can use any interception device in criminal offence cases (including serious violent offences), subject to receiving an interception warrant signed by the Judge of the High Court. Likewise, the Misuse of Drugs Amendment Act 1978[86] permits the New Zealand police to intercept private communica-

tion — subject to a warrant authorized by a Judge of the High Court — in cases involving drug dealing and prescribed cannabis offences (cannabis on a substantial scale). The International Terrorism (Emergency Powers) Act 1987 permits the New Zealand police to intercept private communication during an emergency, again contingent on an authorized warrant[87]. Warrants are valid for no more than 30 days and all intercepted information must be destroyed after proceedings are complete.

The New Zealand Security Intelligence Service Act 1969[88], allows the New Zealand Security Intelligence Service (NZSIS) to carry out electronic interceptions upon issue of an intercept warrant by the Minister in charge of NZSIS and the Commissioner of Security Warrants. The Director of Security can apply for a warrant in cases of threats to national security and/or when needing to gather foreign intelligence information that is essential for security. The warrant is valid for a maximum period of 12 months. The Act was amended twice in 1999 (New Zealand Security Intelligence Service Amendment Act 1999 and New Zealand Security Intelligence Service Amendment (No. 2) Act 1999[89]), allowing NZSIS to install and maintain any equipment or device in the place under investigation and the issuance of foreign interception warrants (where the warrant is issued to intercept communications of a foreign organization or an individual who is neither a New Zealand citizen nor a permanent resident).[90]

Apart from the New Zealand police and NZSIS, the Government Communications Security Bureau (GCSB) — the Signals Intelligence (SIGINT) agency for New Zealand — has the power to intercept private communication and is responsible for both signals intelligence and communications security. The GCSB Act 2003[91] was enacted to specify the provisions by which GCSB can seek a warrant (or authorization for computer access) to protect the country's infrastructure from computer viruses and cyber threats by intercepting the communications of foreign organizations or persons.

The Telecommunications (Interception Capability) Act 2004[92] mandates that network operators and service providers assist surveillance agencies with the interception of telecommunications (phone call and e-mails), subject to an interception warrant from a High Court or under a lawful interception authority. The law ensures that the lawful interception of telecommunications is carried out effectively, and that network operators and service providers do not create any barriers to the introduction of advanced communication technologies. The surveillance agencies include law enforcement agencies (the New Zealand Police or any government department) or an intelligence and security agency (GCSB and Security Intelligence Service).

Deadlines for compliance were also set: For public switched telephone networks, or a telecommunications service, conformance is required within 18 months (the "lead time") from passing of the act; For public data networks, conformance is required within 5 years.

According to the law, network operators have to develop, install, and maintain interception capability across their public telecommunications networks and services. The network operator must also collect call-associated data and intercept telecommunications in a format specified by surveillance agencies (that can be decrypted by them). The operators must also ensure that the interception of telecommunications does not interfere with other communications services. The operators can adopt any network design features and specifications that are appropriate for their purposes.

During the nominated "lead time", costs incurred in developing, installing, and maintaining the interception facility are borne by the Crown in cases where the public switched telephone network or a telecommunications service has been operational before the date on which this Act was introduced as a bill into the House of Representatives (November 5, 2002); otherwise, costs are borne

by the network operator. After the expiration of the lead time, all costs are borne by the network operator. Reminder — the lead time refers to the period beginning from the introduction of the Bill into the House of Representatives and ending either 18 months later in the case of a public switched telephone network or a telecommunications service or five years later for a public data network.

The Telecommunications (Interception Capability) Act 2004 is similar to the US Communications Assistance for Law Enforcement Act (CALEA) 1994 and aligns New Zealand's interception capabilities and regulations with those in countries, such as Australia, the USA and the UK.

85 Source: http://www.legislation.govt.nz/libraries/contents/om_isapi.dll
86 Source: http://www.legislation.govt.nz/libraries/contents/om_isapi.dll?clientID
87 Source: http://www.legislation.govt.nz/libraries/contents
88 Source: http://www.legislation.govt.nz/libraries/contents
89 Source: http://www.legislation.govt.nz/libraries/contents
90 Source: http://www.privacyinternational.org/survey/phr2003/countries/newzealand.htm
91 Source: http://www.legislation.govt.nz/libraries/contents/om_isapi.dll?clientID=1606818175
92 Source: http://www.legislation.govt.nz/

NORWAY

Law Name	Criminal Procedure Act of 1981
Related Legislation	1. Criminal Code 1902 2. Postal and Telephonic Communications Act 1915 3. Telecommunications Act of 1995 4. Electronics Communication Act, 2003
Parties Responsible for Enforcing or Certifying	1. National Telephone Administration 2. Magistrate

In Norway, the Criminal Procedure Act, 1981, (lov om rettergangsmåten i straffesaker 22 mai 1981 nr 25) governs the lawful interception of telecommunications. Other laws that make provision for interception include the Criminal Code 1902, the Postal and Telephonic Communications Act 1915 (lov om kontroll med post- og telegrafforsendelser og med telefonsamtaler 24 juni 1915 nr 5), the Telecommunications Act of 1995 (Lov om telekommunikasjon), and the Electronics Communications Act 2003 (Lov om elektronisk kommunikasjon (ekomloven))[93].

According to the Criminal Procedure Act, wiretapping is permitted under a number of different circumstances. The first is detailed in section 216a which covers narcotics and national security offences. Section 216b covers provisions for wiretapping for less serious offences. In either case, the LEA needs to obtain a warrant from the magistrate court.[94] Under special circumstances, where the need for interception is urgent, section 216d grants that the prosecuting authority may issue an order in court. But subsequent approval for the order must be issued by the court within 24 hours of the warrant being granted.[95] Wiretaps in Norway have a statutory duration of four weeks while section 216f gives permission for a longer period of eight weeks if it is believed that intercepting the communications for four weeks will not be satisfactory. Section 216g mandates that the prosecuting

authority destroy all evidence collected through legal interception at the earliest, appropriate, opportunity.

The Criminal Code 1902 originally prohibited the interception of telephone networks except under special circumstances driven by criminal offences. Moreover, amendments to the Criminal Code prohibited individuals from examining electronic transmission. Later, the Postal and Telephonic Communications Act 1915[96] authorized the government to tap phone lines in cases concerning state security and narcotic drugs offences. The consent for tapping a phone line was provided by the National Telephone Administration.[97]

The Telecommunications Act of 1995 (under Section 9-3) prohibits communication network operators from releasing confidential and private data until an order is provided by the National Post and Telecommunications Authority. Section 7-2 obligates operators to provide unimpeded access to premises where telecommunication equipment is located, failure of which might result in cease and desist orders for telecommunication activity.[98] The Electronics Communication Act of 2003 reiterated the obligation of communication channel operators to maintain privacy of their electronic communications, until such prohibition is set aside by the necessary authorities (tribunal or magistrate) under formal circumstances.[99]

93 Source : http://www.lovdata.no/all/nl-20030704-083.html
94 Source : http://folk.uio.no/lee/publications/Overview_Butterworths.pdf
95 Source : http://www.ub.uio.no/ujur/ulovdata/lov-19810522-025-eng.pdf
96 Source: http://www.ub.uio.no/ujur/ulovdata/lov-19150624-005-eng.pdf
97 Source : http://www.afin.uio.no/forskning/andre_publikasjoner/schengen.pdf
98 Source : http://www.medialaw.ru/laws/russian_laws/telecom/npa/6etr/norv.htm
99 Source : http://www.privacyinternational.org/survey/phr2003/countries/norway.htm

THE PHILIPPINES

Law Name	Republic Act No. 4200 (1965)
Related Legislation	Human Security Act of 2007
Parties Responsible for Enforcing or Certifying	Court

The Republic Act No. 4200, also known as the Anti Wiretapping Act,[100] is the law governing interception of communication in the Philippines. The Act, which came into existence in 1965, prohibits and penalizes wiretapping or interception of any form of communication without proper authorization from the court. Sections 1–4 of the Act cover all aspects of lawfully intercepting communications.

Section 1 of the Act, states that it is unlawful to wiretap or intercept any form of communication, with any device or arrangement, or for any unauthorized person to intentionally possess any record of such communication, unless it is lawfully acquired as evidence for a criminal or civil trial.

Section 2 of the Act assesses the liability of a person who violates the provisions of Section 1. The person is subjected to not less than six months (and no more than six years) of imprisonment. In case the offender is a public official, he/she would be permanently dismissed from government office. In case the offender is an alien, he/she would be subjected to deportation proceedings.

According to Section 3 of the Act, any peace officer, with a written approval/order from the court, can execute wiretapping or possess records of intercepted communications, provided that the identity of the concerned parties and the officer is established and that there are reasonable grounds to prove that the crime has been committed, or is being committed. The reasonable grounds include "the crimes of treason, espionage, provoking war, and disloyalty in case of war, piracy, mutiny in the high seas,

rebellion, conspiracy and proposal to commit rebellion, inciting to rebellion, sedition, conspiracy to commit sedition, inciting to sedition, kidnapping as defined by the Revised Penal Code, and violations of Commonwealth Act No. 616, punishing espionage, and other offenses against national security"[101].

Section 4 of the Act states that any communication/information obtained through violation of the Republic Act No. 4200 shall not be admissible as evidence in any court hearing or investigation.

The Human Security Act of 2007, also known as the Anti-Terrorism Bill (ATB), was passed by the Senate on February 8, 2007, granting power to the government to intercept communications of terrorists. Section 7 of the Act legalizes the surveillance of suspected terrorists and gives authorities the power to intercept or record any communication.[102] Although there are stringent rules and regulations for prohibiting wiretapping, illegal wiretapping continues to remain a problem, and the cases pertaining to wiretapping are constantly increasing across the country.[103]

100 Source: http://www.chanrobles.com/republicactno4200.htm
101 Source: http://www.chanrobles.com/republicactno4200.htm
102 Source: http://www.bulatlat.com/statements/7-3/7-3-atb.htm
103 Source: http://www.privacyinternational.org/survey/phr2003/countries/philippines.htm

POLAND

Law Name	Code of Criminal Procedure, 1997
Related Legislation	1. Police Code 2. *Ministerial draft regulation*, 2001 3. Polish Executive Regulation, 2003 4. *Telecommunication* Act, 2004
Parties Responsible for Enforcing or Certifying	1. Minister of Justice 2. Minister of Interior 3. Court 4. Police

The Code of Criminal Procedure[104], enacted on 6 June 1997, regulates electronic surveillance/wiretapping in Poland. The initial provisions for wiretapping were laid out in the Criminal Procedure Code of 1982.[105]

Under Article 237 (1) of the Code of Criminal Procedure,[106] the police and intelligence services must receive approval from the court before carrying out wiretaps. This authorization may also be provided by the court upon receiving an application from the state prosecutor. The law also specifies those cases in which interception of communications is legal and includes such activities as homicide, kidnapping, hijacking, etc. In cases of exceptional urgency, the state prosecutor may authorize an interception, but the prosecutor is obligated to obtain an authorization from the court within five days. According to Article 238 (1), interceptions are authorized for three months and can be extended for a further three months at most. Courts order that all intercepted communication must be destroyed when it ceases to be of any significance to the criminal proceedings.

Telecommunication and postal service providers are obligated under Article 237 (5) of the Code of Criminal Procedure to ensure that an order for surveillance by the court or the state prosecutor is successfully implemented and such an interception is registered in their records. Only the court or the state prosecutor

is permitted to play the recordings of the interception except in urgent cases where the police, with permission from the court or the state prosecutor, may also play the recordings. The Ministerial Draft Regulation 2001 mandated that ISPs also be able to monitor all appropriate traffic. Moreover, the telecommunication service provider/operator is obligated under Article 165 of the Telecommunication Act[107] 2004, to store all transmission data for at least 12 months; after which this data is deleted or made anonymous.

The Polish Executive Regulation of February 22, 2003, mandates that telecommunications network operators provide access to the information which is transmitted through their telecommunications networks to state security agencies in order to maintain state security and public order.[108] The amendment which was initiated on March 18, 2004 was intended to align the Polish Criminal Code and the Criminal Procedure Code with the Council of Europe's Convention on cyber crime.[109]

104 Source: http://www.era.int/domains/corpus-juris/public_pdf/polish_ccp.pdf
105 Source: www.thepublicvoice.org/events/wroclaw04/adamski.ppt
106 Source: http://www.era.int/domains/corpus-juris/public_pdf/polish_ccp.pdf
107 Source: http://www.mt.gov.pl/viewattach.php/id/d4126689c59347e45b223648e31b10a6
108 Source: http://www.privacyinternational.org/survey/phr2003/countries/poland.htm#ftnref2128
109 Source: http://www.csirt-handbook.org.uk/

ROMANIA

Law Name	1. National Security Law, 1991 2. Police Organization Law, 1994
Related Legislation	1. Criminal Code 2. Law No. 41/1996 3. Law on Anti-Corruption No. 161/2003 4. Emergency Government Ordinance 131/2006, 2006
Parties Responsible for Enforcing or Certifying	1. General Prosecutor 2. Court 3. Serviciul Român de Informatii 4. Serviciul de Informatii Externe 5. Prosecutors Department for Investigations on Organized Crime and Terrorism

In Romania, the interception of postal and telecommunication messages is regulated by the National Security Law, enacted July 29, 1991 (Law No. 51/1991), and the Police Organization Law, dated May 12, 1994 (Law No. 26/1994).[110]

Article 13 of Law No. 51/1991 permits wiretapping in the case of crimes committed against the state. This is authorized by the General Prosecutor of the Office of the Supreme Court.[111] The authorization provided by the General Prosecutor has a maximum duration of six months with a possible extension of a further three months.

Conversely, the authorization granted in conventional criminal cases is limited to 30 days of surveillance. Under Article 17 of Law No. 26/1994, which defines the provisions for countering organized crime, the police can request the prosecutor's office to intercept calls and postal messages.

Article 14 paragraph 2 of Law No. 51/1991 states that the application for authorization has to be made in writing. The public prosecutor will only issue a warrant against the application if probable cause can be justified for the interception. In an

emergency, an intercept can be initiated without authorization, although authorization must subsequently be obtained within 48 hours. The Law also authorizes the Romanian domestic intelligence service, Serviciul Român de Informatii (SRI), and the Romanian foreign intelligence service, Serviciul de Informatii Externe (SIE), to carry out surveillance and interception.

Under Article 91 of the Criminal Code, recordings on magnetic tape could be used as evidence. In 1996, the Criminal Code was amended by passing Law No. 41/1996. This amendment introduced a new section related to the use and conditions under which audio or video recordings may be authorized.[112] Similar provisions for preventing cyber crimes were also introduced by the Law on Anti-Corruption No. 161/2003.[113]

In 2006, Romania adopted a new act — the Emergency Government Ordinance 131/2006 — which was eventually enforced on January 1, 2007, and increased the powers of the Department for Investigations on Organized Crime and Terrorism (DIICOT). According to the press and civil society groups, the prosecutors acting on behalf of the DIICOT will have the authority to monitor bank accounts and IT systems without a warrant. Naturally, the Ministry of Justice has been accused of breaching the right to privacy through this ordinance.[114]

110 Source: http://www.cdep.ro/legislatie/eng/vol42eng.pdf
111 Source: http://www.legi-internet.ro/index.php/Dreptul_la_viata_privata_si_Dr/123/0/?&L=2
112 Source: http://www.itu.int/ITU-D/e-strategies/e-legislation/Doc/Cybercrime_M_Menting.pdf
113 Source: http://www.coe.int/t/e/legal_affairs/legal_co-operation
114 Source: http://www.edri.org/edrigram/number5.2/romania-diicot

SOUTH AFRICA

Law Name	Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002
Related Legislation	1. *Interception and Monitoring Prohibition Act, 1992* 2. Interception and Monitoring Prohibition Amendment Act, 1995
Parties Responsible for *Enforcing or Certifying*	1. South African Police Service 2. *Designated Judge*

South Africa's Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002,[115] regulates the government's interception and monitoring of communications. This law was enacted in December 2002[116] — before this time, the Interception and Monitoring Prohibition Act (1992) governed all aspects of lawful interception. The latter permitted the interception and monitoring of communications and also facilitated the interception of postal articles in cases pertaining to serious crimes or the security of the South African Republic. The legislation was later amended in 1995 under the Interception and Monitoring Prohibition Amendment Act, 1995[117]. A further bill was introduced in the South African Parliament on July 18, 2001 proposing that the Interception and Monitoring Prohibition Act, 1992[118] be repealed and replaced. As a result, the 2002 Act came into existence[119].

The 2002 Act permits the interception and monitoring of certain communications including cellular phones and Internet applications via ISPs. In addition, this law clarifies the procedure for filing an application and issuing a warrant for interception.

The Act also describes the duties of telecommunication service providers (TSPs) and their customers. Chapter 5 of the Law states that all telecommunications service providers, including ISPs, need to make their networks capable of performing interception.

TSPs are required to bear the costs of deploying these capabilities. Criminal penalties may also be brought on service providers that do not comply with the provisions of the Act or do not assist the law enforcement authorities. In addition, TSPs must retain the communications-related data of their subscribers for at least 12 months, with this information being made available to the law enforcement authorities on request.[120]

The interception permit is provided in the form of a warrant issued by a designated judge in response to a written application. This application needs to have an internal departmental approval before application is made to the designated judge. In the case of the South African Police Service, approval is granted by an official who is an Assistant Commissioner or an official of the same rank. In the case of the South African National Defense, the internal approval is provided by an officer rank of Major General. Authorized warrants are valid for a maximum of three months. For cases of exceptional urgency, the application and the authority for interception can be given verbally.

In February 2000, the National Intelligence Agency (NIA) proposed the establishment of a signals intelligence service. This would provide NIA with the authority to intercept all forms of postal, telephone, and Internet communications for the purpose of detecting and preventing criminal offences and strengthening national security. In January 2004, the Department of Communications invited suggestions from technology companies to create centers to assist the interception, monitoring, and storage of e-mail and mobile phone messages.

115 Source: http://www.info.gov.za/gazette/acts/2002/a70-02.pdf
116 Source: http://www.privacyinternational.org/survey/phr2003/countries/southafrica.htm
117 Source: http://www.info.gov.za/acts/1995/a77-95.pdf
118 Source: http://www.privacy.org/pi/countries/south_africa/sa-interception-act-1992.txt
119 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005peru-sril.pdf
120 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005peru-sril.pdf

SWEDEN

Law Name	1. *Criminal Procedure Code* 27:18 2. Criminal Procedure Code 27:19
Related Legislation	1. Bill 2002/2003:74 2. Act 1996:416 3. Law of Secret Camera Surveillance (Paragraph 1) 4. Telecommunications Act, 1993 5. International Legal Assistance in Criminal Matters Act, 2000 6. Electronic Communications Act, 2002
Parties Responsible for Enforcing or Certifying	1. Police 2. Prosecutor

In Sweden, lawful wiretapping and wire surveillance is regulated by the Criminal Procedure Code 27:18 and Criminal Procedure Code 27:19, respectively. Wiretapping is defined as the interception of communication through telephone or fax. Wire surveillance is defined as the gathering of information regarding the number of messages sent from or to a specific telephone number and its time and duration. Camera surveillance is regulated in paragraph 1 of the Law of Secret Camera Surveillance and is used for investigative purposes.[121] Other statutes making provisions for lawful interception of telecommunications include the Telecommunications Act[122] (1993:597) of 1993, the International Legal Assistance in Criminal Matters Act[123] (2000:562) of 2000, and the Electronic Communications Act[124] (2002/03:110) of 2002.

Under the Criminal Procedure Code, the interception of communications is enforced by the police after obtaining a court order or warrant on the basis of a prosecutor's application. All permitted interceptions can only be used to aid the police in their investigations and for constructing a [prosecution] case. Telecommunication interceptions are valid from a minimum of 1 day to a maximum of 11 months, while camera surveillance usually lasts for no more than 29 days. Telecom operators are bound to

provide decrypted signals to authorities if required and to retain all traffic data generated through telephony or the Internet. The period of data retention may vary from a minimum of one year to a maximum of three years.[125]

In 1996, the Telecommunications Act was passed and obliged telecommunication service providers to maintain the privacy of the entire interception process while simultaneously providing the intercepted communication to law enforcement. The Telecommunications Act was eventually replaced by the Electronic Communications Act of 2002, which obligates all electronic networks and service providers to assist authorities with the process of wiretapping. This Act was eventually enforced on July 25, 2003.

The International Legal Assistance in the Criminal Matters Act makes provisions for the interception of communications of suspected criminals in Sweden and abroad. While the authorization for interception has to be provided by a prosecutor or a court, this Act also provides prosecutors with the authority to request legal assistance abroad. Chapter 4 (Sections 25–28) lists provisions for the interception of communications through wiretapping, telecommunications surveillance, and camera surveillance.

In 2003, the Swedish government approved Bill 2002/2003:74, which made it possible to lawfully intercept communications to investigate a number of crimes, such as murder, kidnapping, hijacking, etc. The new Act on Criminal Responsibility for Terrorist Crimes[126] also empowered the police to intercept and use secret surveillance techniques to monitor criminal behavior. This Act was enforced in July 2003.

New legislation has also been proposed due to increased incidents of crime and terrorism in Sweden. This legislation will offer the National Defence Radio Establishment (FRA) the authority to tap cross-border Internet traffic and phone calls without a court order. The law grants authorization to the police to use data min-

ing software to flush out data communications based on keyword search. However, communications within Sweden would not be affected by this legislation. If approved, the law will come into effect from July 1, 2007.[127]

During 1988 to 1996, the number of permitted wiretap cases ranged from 210 to 333.[128] In 2002, the number of cases increased to 533. Based on its relatively small population, Sweden was listed in third position with respect to the number of intercepts per inhabitants; in 2003, this ratio was 33 intercepts per 100,000 inhabitants. Only Italy and the Netherlands are ahead with 76 and 62 intercepts per 100,000 inhabitants, respectively.[129]

121 Source: http://www.ihf-hr.org/viewbinary/viewdocument.php?doc_id=5537
122 Source: http://www.medialaw.ru/laws/russian_laws/telecom/npa/6etr/swed.htm
123 Source: http://www.sweden.gov.se/content/1/c6/01/52/68/db667afc.pdf
124 Source: http://www.sweden.gov.se/content/1/c6/01/84/54/5ae98894.pdf , http://pts.se/Archive/Documents
125 Source: http://www.privacyinternational.org/survey/phr2005/PHR2005swed-ven.pdf
126 Source: http://www.isp.se/documents/public/se/pdf/lagar/2003_148e.pdf
127 Source: http://cybrinth.com/uploads/031407%20Plain.doc
128 Source: http://cryptome.org/se-crypto99.htm
129 Source: http://www.smartmobs.com/archive/2007/03/07/electronic_surv...html

THE UNITED KINGDOM

Law Name	Regulation of Investigatory Powers Act 2000
Related Legislation	1. The Interception of Communications Act of 1985 (Section 2) 2. The Interception of Communications Act of 1988 3. Police Act 1997 4. The Interception of Communications Act of 2001 5. The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002 6. Wireless Telegraphy Act 1949
Parties Responsible for Enforcing or Certifying	1. Secretary of State 2. Interceptor

In the UK, Section 2 of the Interception of Communications Act of 1985 laid the recognized foundation for lawful interception. This Act amended section 45 of the Telecommunications Act 1984. Three years later, the Act of 1985[130] was also modified so that it was in accordance with the Telecommunications (Interception) Act of 1979 of the Commonwealth. The modified Act, The Interception of Communications Act of 1988,[131] detailed the responsibilities of the police force, the office of police integrity, and special investigations monitoring. The Interception of Communications Act 2001[132] was a further modification of the 1985 version and dealt with issues encompassing the scope of warrants.

The Regulation of Investigatory Powers Act 2000[133] or RIPA is the primary legislation that now monitors and regulates the lawful interception of communications in the UK. It permits the Secretary of State to issue warrants authorizing the interception of postal services or a public telecommunications system in case of any threat to national security or for preventing or detecting criminal activities.

RIPA came into force on October 2, 2000 after the UK government realized the need for improved legislation to cover developing aspects of lawful interception. The new requirements were reflected in a consultation paper published in 1999. RIPA now describes the procedures of applying for and issuing a warrant. Only the heads of law enforcement agencies and their representatives are eligible to apply for interception warrants. These are then issued by the Secretary of State. The intercepted telephony data and subscriber information must be retained for 12 months while SMS, EMS, MMS, e-mail, and ISP data need only be retained for six.[134]

RIPA also describes the contents, duration, cancellation, and renewal requirements for warrants. Though the effective period of all new warrants is the same, it may vary if renewed. Of note, the tapped material cannot be used as legal evidence except under specific circumstances. RIPA also modified wiretapping to include all forms of telecommunications, vis-à-vis e-mails, chat, Web surfing, and Internet service, and made the tapping of private networks lawful as well. RIPA also empowered LEAs to serve notice to convert encrypted data to the readable or decrypted format; although this title has not been implemented at present.

The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002[135] defined the obligations of the public postal and public telecommunications service providers in accordance with RIPA. It was enforced on August 1, 2002. These obligations, however, do not apply to those telecom service providers who provide service to less than 10,000 people in the UK.

According to the provisions in the 2002 Order, telecom service providers need to enable an intercept within one working day of receiving a warrant. The service provider needs to ensure the completeness and near real-time transmission of intercepted data to the authorities. In addition, the transmission of both the intercepted and related communication data needs to be guaran-

teed. The handover interface needs to follow industry standards such as those prescribed by the European Telecommunications Standards Institute (ETSI).

The telecommunications service provider must only filter the traffic data for the target subscriber. In addition, the capability must exist for the simultaneous interception of 1 in every 10,000 subscribers. Moreover, the service provider needs to ensure that the reliability of the interception being carried out is at least equal to the telecommunication service which would be transmitting the intercepted communication. The interception capability can be audited; as a result, the premises are named in the warrant. The telecom service provider also needs to guarantee the secrecy of the intercept process.

The Interception Code of Practice[136] lays down the procedure that must be followed before the process of intercepting communication. The Police Act 1997[137], Part III, Section 92, makes provisions for intercepting wireless telegraphy while Section 93 deals with powers for authorization.

Under RIPA, 1,983 and 1,973 warrants for lawful interception were issued in 2003 and 2004, respectively, in England and Scotland. In addition, there were 3,367 modifications of warrants in 2004 as compared to 2,844 modifications in 2003.[138] Although the UK law enforcement agencies made 439,054 requests for communications data during January 2005-March 2006, only 2,407 requests were permitted for content-based lawful interceptions. In addition, there were 5,143 requests for modifications, aggregating the overall to 7,550.[139]

130 Source: http://www.swarb.co.uk/acts/1985InterceptionCommunicationsAct.shtml
131 Source: http://www.austlii.edu.au/au/legis/vic/consol_act/tpa1988556/
132 Source: www.gov.im/lib/docs/infocentre/acts/ica2001.pdf
133 Source: http://www.opsi.gov.uk/Acts/acts2000/20000023.htm
134 Source: http://en.wikipedia.org/wiki/Data_retention
135 Source: http://www.opsi.gov.uk/SI/si2002/20021931.htm
136 Source: http://www.minez.nl/
137 Source: http://www.opsi.gov.uk/acts/acts1997/1997050.htm
138 Source: http://www.statewatch.org/news/2005/nov/uk-tel-tap-rep-2004.htm
139 Source: http://www.statewatch.org/news/2007/feb/07uk-teltap-2005-2006.htm

THE USA

Law Name	1. Communications Assistance for Law Enforcement Act (CALEA): The law was introduced in 1994 2. Title II of USA Patriot Act, 2001 3. Foreign Intelligence Surveillance Act (FISA) of 1978 4. Title III of Omnibus Crime Control and Safe Streets Act of 1968
Related Legislation	1. The Wire and Electronic Communications Interception and Interception of Oral Communications Act 2. The Electronic Communications Privacy Act[140]
Compliance Deadlines	Communications Assistance for Law Enforcement Act (CALEA) • Original deadline of 25 October 1998 • Deadline extended to 30 June 2000 • Extension of deadline from 30 September 2001 to 19 November 2001 for CTIA[141] • ISPs compliance deadline of 14 May 2007[142]
Parties Responsible for Enforcing or Certifying	Predominantly, the FBI
Impacted Parties	Common carriers, facilities-based broadband Internet access providers, and providers of interconnected Voice over Internet Protocol (VoIP) service[143]

In the US, four main laws — the Communications Assistance for Law Enforcement Act (CALEA), Title II of USA Patriot Act of 2001, the Foreign Intelligence Surveillance Act (FISA) of 1978, and Title III of the Omnibus Crime Control and Safe Streets Act of 1968 — cover most of the nation's lawful interception statutes. While Title III of the Omnibus Crime Control and Safe Streets Act legislates lawful interception for domestic law enforcement purposes, the Foreign Intelligence Surveillance Act covers wiretapping for intelligence purposes where the subject could be a foreign (non-

US) person working as an agent on behalf of a foreign country. In 1994, the US Congress enacted CALEA to further clarify the statutory obligation of telecom carriers to maintain network infrastructures that assist law enforcement agencies with electronic surveillance. Moreover, post the 9/11 terrorist attack, Congress furthered electronic surveillance authorities under the USA PATRIOT Act. Provisions made under this act served mainly to broaden those already defined under FISA.

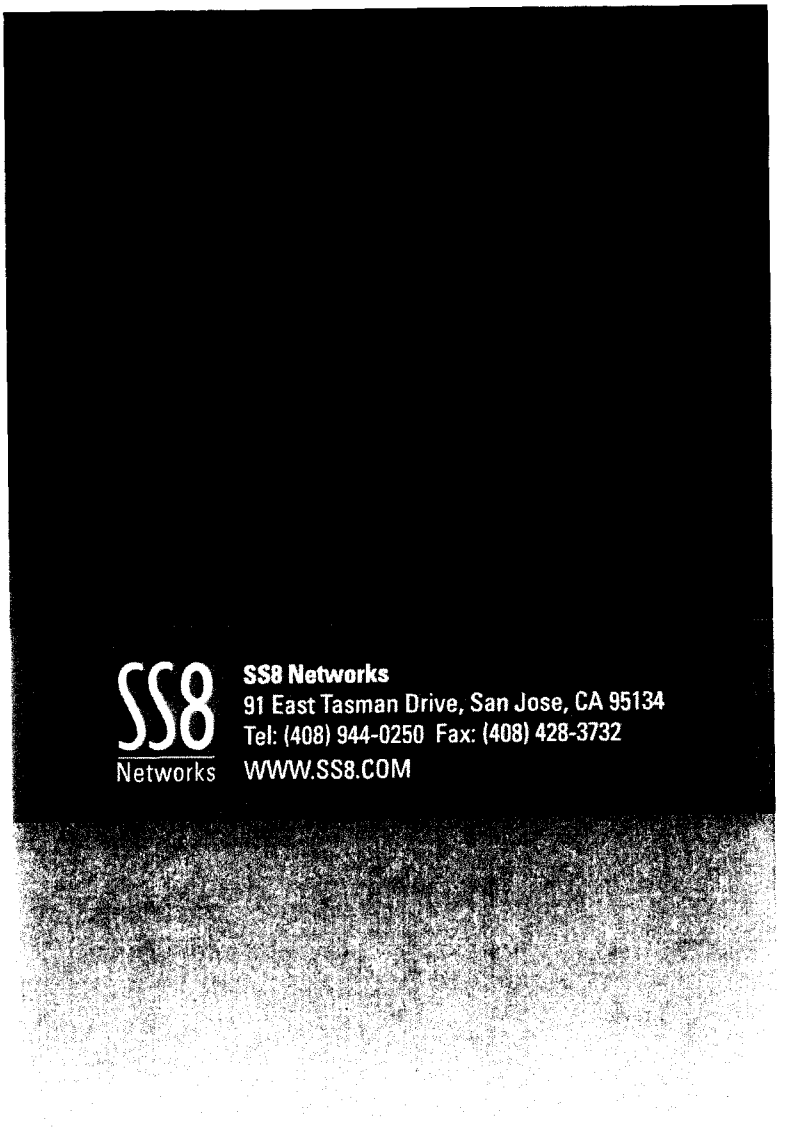
To guide carriers through the many laws covering legal interception in the US, telecom operators can look to CALEA as the legislation that most succinctly clarifies their obligations. The law was introduced in response to concerns that emerging technologies were creating difficulties for law enforcement agencies to execute authorized surveillance, and that a more standardized process was required.

According to the provisions of CALEA, a telecom carrier is required to design and maintain capabilities that allow customer traffic and signalling to be expeditiously and unobtrusively isolated, then forwarded to LEAs in a standardized manner to possibly multiple LEA locations (other than the premises of the carrier).[144] CALEA included a reimbursement clause, which allowed telecom operators to be repaid for the costs incurred in making their equipment, facilities, and services compliant with the requirements of CALEA if the equipment was installed pre-1995. A fund was set aside to support the upgrades of pre-1995 equipment, but the cost for post 1995 equipment compliance fell to the service provider.

The USA PATRIOT Act was a legislation milestone that significantly broadened the scope of federal electronic surveillance. The Act has added terrorist, computer fraud, and financial offences to the list of activities that can secure Title III wiretaps. The law also permits the use of roving wiretaps for foreign surveillance on US soil and expands the use of traditional pen register or

trap and trace devices from "call processing" to "the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications. Multi-jurisdictional warrants may also be obtained for wiretapping purposes, making it easier to track criminals across borders.[145]

140 Source: http://www.ncsl.org/programs/lis/CIP/surveillance.htm#Federal
141 Source : http://www.fcc.gov/Bureaus/Common_Carrier/Orders/2001/fcc01265.txt
142 Source : http://www.dslreports.com/shownews/83607
143 Source: http://www.fcc.gov/calea/
144 Source: http://en.wikisource.org/wiki/Communications_Assistance_for_Law_Enforcement_Act_of_1994
145 Source: http://www.fas.org/irp/crs/RL30465.pdf


SS8
Networks
SS8 Networks
91 East Tasman Drive, San Jose, CA 95134
Tel: (408) 944-0250 Fax: (408) 428-3732
WWW.SS8.COM

LISTE DES ADMs - LAWFUL ACCESS (2007-09-20)

Mr. Brian Saunders
Assistant Deputy Attorney General
Federal Prosecution Service
Department of Justice
284 Wellington Street, Room 2119
Ottawa, Ontario K1A 0H8

Brian.saunders@justice.gc.ca (957-4756)

(Francine Lance : 957-4757)

Assistant Commissioner Bruce Rogerson
Director
Technical Operations Directorate
RCMP
1426 St-Joseph Blvd
Gloucester, Ontario K1A 0R2

Carole.routhier@rcmp-grc.gc.ca

(Carole Routhier : 993-1619)

Rennie Marcoux
Assistant Secretary to the Cabinet
Privy Council Office
Security and Intelligence
59, Sparks Street, room 307B
Ottawa, Ontario K1A 0A3
(957-5386)
rmarcoux@pco-bco,gc,ca

(Sylvie Forcier : sforcier@pco-bcp.gc.ca (957-5386)

Scott Broughton
A/Senior Assistant Deputy Minister
Public Safety Canada
Office of SADM
269 Laurier Avenue West, Room 17A-1400
Ottawa, Ontario K1A 0P8
(991-2820)

Anne-Marie Doupagne (991-2819)
Anne-marie.doupagne@ps-sp.gc.ca

Ron Parker
Visiting Senior Assistant Deputy Minister, Industry Canada
Strategic Policy
235 Queen Street
1019A, East Tower
Ottawa, Ontario
K1A 0H5

Julie Malboeauf
(613) 947-3023

Mr. Michael Devaney
DG, Policy and Communications
Communications Security Establishment
719 Heron Road
Ottawa, Ontario K1A 0K2

michael.devaney@CSE-CST.GC.CA;
991-7140

tammy.varin@cse-cst.gc.ca (991-7254)

Mr. Ted Flanigan
Assistant Director Intelligence
Canadian Security Intelligence Service
1941 Ogilvie Road
Gloucester, Ontario K1J 1B7

flanigant@smtp.gc.ca (842-1487)

(Brigitte Henrie: 842-1210 ou Christine Warias 231-0652)

Michael M. Binder
Assistant Deputy Minister, Industry Canada
Spectrum, Information Technologies
And Telecommunications
300, Slater Street
Jean Edmonds Tower North, room 2035B, Floor 20
Ottawa, Ontario K1A 0C8

St-Jacques.Janet@ic.gc.ca
(Janet St-Jacques: 998-0368)

Ms. Sheridan Scott
Commissioner of Competition
Industry Canada
Competition Bureau
Place du Portagem Phase I, Floor 21, Zone 4
50 Victoria Street
Hull, Québec K1A 0C9

Diotte.Suzanne@cb-bc.gc.ca
(997-5300)

Donald K. Piragoff
Senior Assistant Deputy Minister
Department of Justice Canada
284 Wellington Street, EMB-50195
Ottawa, Ontario K1A 0H8

Chantal Pelchat (957-4726)

From: DiFrancesco, Janet: SITT-STIT
Sent: Thursday, August 27, 2009 8:08
To:
Subject: FW: Response to Concerns Regarding Bill C-47

Dear

Thank you for your correspondence of June 19, 2009, regarding your concerns with Bill C-47, *An Act Regulating Telecommunications Facilities to Support Investigations*.

My colleague, the Minister of Public Safety, the Honourable Peter Van Loan and I have sought the input of many stakeholders including the telecommunications industry prior to tabling this important legislation.

I assure you we have and will continue to consult with stakeholders including the telecommunications industry and privacy stakeholders to ensure that this legislation is consistent with Canada's privacy policies and rules, and does not place a financial burden on the telecommunication service providers.

This bill is intended to bring law enforcement officials access to information into the digital age. In the past, law enforcement authorities relied on the phone book and other similar directories to obtain subscriber information. With the development of the Internet and widespread access to wireless and other communications devices, there are currently many gaps in the information available to law enforcement and other government authorities.

It is also important to note that the rules regarding judicial oversight of all intercept warrants are not changing as part of this legislation.

In order to protect telecommunications service providers from economic burden, the proposed legislation would also empower the Governor in Council, on the recommendation of both the Ministers of Public Safety and Industry, to exempt companies from all of the requirements of the Act for up to two years. The exemption mechanism is provided because the requirements of the legislation are complex and technical and there is a need to provide a 'safety valve' to deal with special circumstances after it comes into force.

I will continue to follow the developments of this legislative initiative as it proceeds through the parliamentary process and will continue to ensure that the legislation does not affect the competitiveness of our telecommunications industry or unduly infringe on Canadians privacy.

Sincerely,

INTERNET

To: [redacted]

Dear [redacted]

Thank you for your correspondence of June 19, 2009, regarding your concerns with Bill C-47, *An Act Regulating Telecommunications Facilities to Support Investigations*.

My colleague, the Minister of Public Safety, the Honourable Peter Van Loan and I have sought the input of many stakeholders including the telecommunications industry prior to tabling this important legislation.

I assure you we have and will continue to consult with stakeholders including the telecommunications industry and privacy stakeholders to ensure that this legislation is consistent with Canada's privacy policies and rules, and does not place a financial burden on the telecommunication service providers.

This bill is intended to bring the access of law enforcement officials to information into the digital age. In the past, law enforcement authorities relied on the phone book and other similar directories to obtain subscriber information. With the development of the Internet and widespread access to wireless and other communications devices, there are currently many gaps in the information available to law enforcement and other government authorities.

It is also important to note that the rules regarding judicial oversight of all intercept warrants are not changing as part of this legislation.

In order to protect telecommunications service providers from economic burden, the proposed legislation would also empower the Governor in Council, on the recommendation of *both* the Ministers of Public Safety and Industry, to exempt companies from all of the requirements of the Act for up to two years. The exemption mechanism is provided because the requirements of the legislation are complex and technical and there is a need to provide a 'safety valve' to deal with special circumstances after it comes into force.

I will continue to follow the developments of this legislative initiative as it proceeds through the parliamentary process and will continue to ensure that the legislation does not affect the competitiveness of our telecommunications industry or unduly infringe on Canadians privacy.

Sincerely,