BILETA

16th BILETA Annual Conference

April 9th - 10th, 2001.
University of Edinburgh, Scotland.

A Tale of Two Interception Regimes: RIP v CALEA, a comparison.

GAVIN SUTTER
(Queen Mary and Westfield)

---

1. Introduction

That there should be lawful interception of electronic communications, for example, to investigate child pornography trafficking, receives broad support from both communication service providers and law enforcement. Both stress the importance of legislation being up to date: technological development will not wait for law to catch up. Communication Service Provider (CSP) interests place strong emphasis on the desirability of laws that set out exactly what terms such as interception mean.

In the USA and the UK much the same arguments are put: LEAs are by and large in favour of wider investigatory powers, while CSPs - "telecommunications carriers" in the language of the US legislation - are of the opinion that the level of technical assistance which the FBI, for example, are seeking is unfeasible. The question of costs is also a matter of dispute between those groups.

2. US & UK Interception of Electronic Communications Regimes

The USA is somewhat ahead of the UK in the provision of a legislative regime designed to accommodate the interception of electronic communications. The latest Act regulating interception to be passed by Congress is the Communications Assistance for Law Enforcement Act (CALEA), 1994[1]. There is some dispute as to the key intention of the Act. The FBI, for instance, takes the view that CALEA was enacted "to ensure that technological changes in the industry would not compromise the ability of law enforcement agencies to engage in lawful electronic surveillance."[2]

LEAs focus mainly on CALEA's adaptation of the law on wiretapping to embrace these latest

technologies in order to prevent them from becoming channels for the planning and commission of organised crimes. Rights and CSPs prefer to emphasise the limitations placed upon electronic surveillance by CALEA, designed to protect individual privacy.

Interception in the UK was, from 1985, governed by the Interception of Communications Act, however, that Act had been outdated by technological advances such as the Internet, the proliferation of mobile telephony and social trends in the increased usage of such technologies, largely unforeseen at the time of its passage. The Regulation of Investigatory Powers Bill was introduced in the UK in early 2000, and passed into law during July the same year. It aims to bring UK interception law into line with technology as well as to bolster the effectiveness of LEA investigations by redrawing and clarifying the (legal) relationship between CSPs and LEAs.

The main thrust of the US legislation is to oblige CSPs to assist LEAs to carry out an interception on their networks in furtherance of a criminal investigation. Under section 103, CALEA imposes four main obligations upon those to whom it applies[3]:

* A telecommunications carrier must ensure that its network facilities are capable of enabling the interception of content of data communications from a particular individual.

* The telecommunications carrier must also provide the capability to isolate the `call-identifying information' associated with a particular individual.[4]

* Such information is required to be passed on to LEAs when a request for same has been authorised by the appropriate court order.

* Interceptions must be carried out in as unobtrusive a manner as possible so that the target will not be made aware of the surveillance and the privacy of other communications on the same telecommunications network is assured.

Section 104 of CALEA obliges the US Attorney General to draw up a list of the maximum capacity requirements, i.e. the actual number of simultaneous interceptions, which a telecommunications carrier can be obliged to carry out for LEAs.

The UK Regulation of Investigatory Powers Act introduces a similar regime. So far as is here relevant, section 12(1) provides that:

"The Secretary of State may by order provide for the imposition by him on persons who-

(a) are providing...public telecommunications services, or

(b) are proposing to do so,

of such obligations as it appears to him reasonable to impose for the purpose of securing that it is and remains practicable for requirements to provide assistance in relation to interception warrants to be imposed and complied with."

Capacity requirements set by the Secretary of State under this discretionary power are to be communicated to those subject to the obligations by notice (section 12(2)). This notice will also specify a date for compliance, set as "such period as appears to the Secretary of State to be reasonable as the period within which the steps specified or described in the notice are to be taken." (section 12(8)).

3. Capability / Capacity: Feasibility

CSPs raise objections to orders obliging modification of networks to facilitate interceptions on grounds of feasibility and cost. UK CSP interests have argued, for instance, that the volume of intercepted data which law enforcement bodies regard as desirous must be limited in order that the service a CSP is able to offer it's clientele is not restricted. A recurring theme in CSP statements on the subject is the need for much consultation between government bodies responsible for new regimes and the industries likely to be affected. Clear definitions as to what exactly may be expected are demanded. CSPs are concerned that, as BT has expressed it, "[t]here should be no provisions requiring CSPs to collect, store or manipulate data for the Law Enforcement agencies...other than that gained in the normal course of business."[5]

It is emphasised that while clear definitions are essential, these should be formulated on the basis of function rather than rapidly evolving technology. Technological definitions would date rapidly, confounding the usefulness of the power to intercept. When new legislative regimes are being created, CSPs are keen that they are protected from unwittingly carrying out an unauthorised interception; for example by carrying out routine monitoring of their own networks without an interception warrant.

The RIP Act goes some way towards answering these issues, but does not answer others. Good functionality-based definitions are given for "interception" (section 2(2)), for instance, which would seem sufficient to accommodate routine interceptions (see sections 3 and 4). However, the Act lacks any form of provision setting out precise functional requirements as to the level of interception capacity that will be expected. Section 12 places the responsibility for setting these standards upon the Secretary of State, standards to be set out in an Order presented to a CSP under this section. As of yet, no such Orders have been issued.[6] The feasibility of the UK requirement to provide an interception capability will be determined by the capacity requirements which the Secretary of State sets out. The position in the USA is not much further on. CALEA placed similar requirements on the US Attorney General, under Section 104. The Attorney General delegated this responsibility to the FBI, which published an Initial Notice of Capacity in 1995 for local exchange, cellular, and broadband personal communications services (PCS) carriers. These standards were rejected by the industry, which continues to oppose the implementation of such requirements as are made under section 104 on grounds of feasibility and cost. In December 1997, the telecommunications industry, in the face of objections from LEAs, adopted an interim technical standard known as J-STD-025. LEAs were of the opinion that this did not go far enough to satisfy CALEA's requirements on protection of public safety and national security. The debate has continued over the last several years: most recently the FCC has published it's Third Report and Order (FCC 99-230) on assistance capability requirements. The FCC concluded that, in addition to the J-STD-025 standard already adopted by the industry, six capabilities that the Department of Justice and the FBI had pushed for should be met by the industry in order to comply fully with CALEA, as follows:

* Content of conference calls initiated by the interception-target

* Information identifying whether a party to a conference call is on hold, has joined or been dropped from the conference call

* The target's use of features such as call-forwarding, call waiting, call hold, and three-way calls, information obtainable via accessing target-initiated dialling and signalling information.

* In-band and out of band signalling (notification message) - An LEA will be notified when a target's service sends a network message, e.g. a tone, to the target or associate

* Timing Information permitting the LEA to match `call-identifying information'[7] with the content of an intercepted call.

* Dialled digit extraction - i.e. the provision of any digits dialled by a target after connecting to

another telecommunications carrier's service. Some of these digits will fall under the heading of call-identifying information[8]

Further capabilities sought by the FBI were rejected by the FCC.

The issue of interceptions *capacity* in the USA is also far from settled, as a consortia of rights groups have mounted legal challenges to what they regard as the unwarranted invasion of privacy which these requirements in the Third Report and Order represent.

The practicalities of the international character of many telecommunications networks are not fully addressed in either CALEA or RIP. Provision is made to cover situations that may arise when an interception in another jurisdiction becomes necessary. For instance, a user in the UK might be accessing the Internet via a UK ISP but the most appropriate place for the actual interception could be in the USA. Physical location aside, it is a reality of the CSP industry that much of the equipment is manufactured in the USA. Inevitably this means that it will generally be manufactured to US legal standards of design and function where interception equipment is concerned: the question then arises as to whether this will have an effect on a CSP's ability to comply with UK legal requirements, or whether any additional cost in making the equipment so compliant will render it prohibitively expensive in commercial practice. In the USA, a date for full compliance with the capability and capacity requirements under CALEA was set at June 30, 2000. However, while the FCC was determined to stick to this deadline, several telecommunications companies voiced the opinion that it was not feasible as their equipment suppliers were unlikely to meet this deadline. The potential knock-on effect of such factors elsewhere - such as in the UK - given that the majority of such equipment in production is manufactured in the USA, is significant. If, however, the telecommunications industry - in many ways a *global* industry - can in future meet some form of standard which is likely to be adopted internationally, the situation may well change. The debate is likely to rumble on for some time to come, however, particularly in the US where the issue of individual privacy is paramount. The so-called "Carnivore" interception system used by the FBI continues to draw criticism for being overly invasive, while in a recent decision the Federal Court of Appeals for the District of Columbia rejected certain FBI demands for additional surveillance powers. In a unanimous decision, the court held that the Federal Communications Commission's requirement that telecommunications carriers must provide interceptions capacity in their networks for the facilitation of law enforcement investigations was "an entirely unsatisfactory response" to the privacy rights recognised within CALEA. In placing these requirements upon the industry, the court held, the FCC also failed to take into account the financial cost to telecommunications carriers. One of the additional features which the court rejected as too invasive was the ability to extract any dialled digits from a call, which might include a long distance telephone number - call-identifying information - or bank account or banking or credit card details - clearly content.[9]

What effect might roaming agreements between CSPs in different countries have? For example, a client registered with a UK CSP may physically be in France, say, using his account with that company via a French company's network, as per a roaming agreement between the two CSPs. If an interception of data transmitted thus is to be carried out, how far can the UK CSP be expected to have access to data transferred not over its own network but that of its French counterpart?

This is an area which is likely to become increasingly significant as wireless application protocol (WAP) enabled mobile telephones and in turn third generation cellular phones become readily available to consumers, allowing them to access the internet via the cellular network. Clearly the most appropriate means of regulation will have to be tied to a set of internationally agreed standards. The Internet Engineering Task Force (IETF), an influential technical consortium, has expressed itself to be opposed to the introduction of "functionality designed to facilitate wiretapping."[10]

Telecommunications providers in both the USA and the UK also place great importance upon the cost associated with providing interceptions capacity and assistance. The cost has been estimated to

be high: Demon Internet has given an approximate figure of between 10% and 15% of its total revenue. Should a CSP be required to supply the intercepted information to more than one investigating agency, the systems required to be put in place will be more complex and costly. As the London Internet Exchange (LINX) has put it, this is unlikely to prove a "once-off" expenditure: as technology evolves networks must be replaced and so interception equipment will require to be sympathetically updated. The speed of future network design and development could potentially be retarded by the requirement to build new systems around an obligation to include interception facilities. One possible approach suggested by the Internet Service Providers' Association (UK) is to grant a grace period of six months in order to prevent new technology from being held back from release while interception capacity is added. Such an approach is taken in Holland, where Dutch law provides a nine-month exemption before compliance becomes obligatory. However, this is only a solution during the immediate period after such a requirement is introduced - in the longer term the same problem may recur.

Interception inevitably raises issues of interception versus user-privacy: in the event that the provision of an intercept facility conflicts with previous privacy policies that CSPs' customers have signed up to, the CSPs will encounter the expense of redrafting such policies and renewing agreements with their clients. These costs could prove prohibitive for small scale internet service providers (ISPs), for instance. It might be argued, then, that regulations should be relaxed for such companies, however, this would merely drive criminal elements to seek out and use smaller ISPs where their communications would be much less likely to be intercepted.

Larger CSPs may also struggle with costs of maintaining an interception facility over vast networks that are much more complex and less flexible than smaller concerns. UK service providers could well face significant disadvantages as regards their competitors operating from jurisdictions that do not impose these obligations. CSP interests are keen to point out that such expenditure should be met by investigating agencies as it would not arise in the normal course of business, only to facilitate their investigations. The ISPA (UK) has gone so far as to state that the investigating authorities, or government directly, should at the very least pay for the maintenance and use of mandatory interception facilities.

Some provision is made under both regimes to the effect that the full cost need not be borne by the individual CSP in seeking to comply with the relevant standard capacity. The UK RIP Act provides that, where an order to provide internet capacity is made, the Secretary of State will also decide upon an "appropriate contribution"[11] to be made by the government towards the cost of compliance. The issue of cost of human resources involved in interceptions may also be the cause of much debate: will this be included under the "appropriate contribution"? What will no doubt prove the most controversial area in the UK, however, will be whether the example of the US legislation will be followed in relation to what will be expected of CSPs where no government funding is forthcoming in order to meet the costs of attaining the standard to be set by the Secretary of State.

In the USA, there is limited provision made for the reimbursement of telecommunications carriers' expenses in achieving compliance with CALEA:

"the Attorney General may, subject to the availability of appropriations, agree to pay telecommunications carriers for all reasonable costs directly associated with the modifications performed by carriers in connection with equipment, facilities, and services installed or deployed on or before January 1, 1995, to establish the capabilities necessary to comply with section 103."[12]

Whether this was reasonably achievable as regards equipment, facilities or services installed or deployed after that date in individual cases will[13]ultimately be determined by the FCC. Factors taken into account in such cases are to include the effect on public safety and national security, privacy protection, cost-effectiveness, avoiding retarding technological progress, and so on. LEAs wished to stick rigidly to the provisions of CALEA on this matter, however, the industry position is

that all costs incurred as a result of CALEA compliance should be recoupable. Of great interest from a UK standpoint is section 109(d), which provides that, as regards qualifying facilities and services,

"if a [telecommunications] carrier has requested payment in accordance with procedures [set out in CALEA], and the Attorney General has not agreed to pay the telecommunications carrier for all reasonable costs directly associated with modifications necessary to bring any [qualifying] equipment, facility or service ... into compliance with the assistance capability requirements of section 103, such equipment, facility or service shall be considered to be in compliance with the assistance capability requirements of section 103 until the equipment, facility, or service is replaced or significantly upgraded or otherwise undergoes major modification."

Such a provision would be extremely popular with the UK industry, still pressing for all costs associated with compliance to be met as a condition of the finalised legislation arising out of the RIP Act. It would, of course, also provide a strong incentive to government to ensure that all CSPs required to comply receive adequate compensation in order that safe-havens are not provided for those wishing to use electronic communications for criminal purposes.

4. Procedure

CSPs in the UK tend to perceive law enforcement bodies, and particularly the police, as lacking in technological expertise: law enforcement expressions of what is desirous in an interception regime are regarded as unfeasible primarily due to a lack of understanding of the current state of the art and its limitations. CSPs call for investigatory authorities to develop not only the level of technical expertise necessary to comprehend the situation clearly, but also to be able to deal with the processing of information and data provided by a CSP involved in an interception. Necessary training should be facilitated by the investigatory authorities themselves, say CSPs. The situation in the USA is broadly the same, with industry opinions being preoccupied with feasibility and cost issues rather than the procedural mechanics of interception warrants.

Some hope is offered in the UK by the inclusion of section 13 in the RIP Act, which provides for the creation of a Technical Advisory Board to advise on interception matters. It is not yet clear exactly how such a board will operate in practice, to what purpose it will be put or what weight its decisions or advice will carry, however, it is clearly a step in the right direction, including, as it does, provision that the interests of both those given responsibilities (section 13(2)(a)) and those granted powers (section 13(2)(b)) should be represented equally (section 13(2)(d)).

Investigatory authorities tend, as might be expected, to be less concerned with the technological details, being more interested in the procedure which should be followed for the issue of an interception warrant. Issues raised here include questions such as on whose authority an interception may be issued: is the appropriate body for doing so ministerial or judicial? Or part of the investigating authority itself? There is some discussion as to whether the renewal of an interception warrant should require authorisation at the same level as its original issue, or whether this can be done by a subordinate authority. Such a proposal is, of course, rooted in the belief that interceptions will become more common as electronic communications become more pervasive in society - not a view which all LEAs share. A highly significant issue is that of the actual targeting of a warrant. Investigatory authorities, as well as CSPs, express a preference for an approach which permits the targeting of an individual rather than a specific address, an important distinction given that an individual may now use multiple telecommunications - mobile telephones, web-based messaging services, multiple email addresses, etc.

RIP makes no change to the 1985 Interception of Communications Act's requirement of ministerial authorisation for an interception warrant - section 7 of the Act specifies the requirement of the

Secretary of State's authorisation. This is in contrast to the US system's requirement of *judicial* authority under CALEA. Section 6 of the RIP Act sets out those who may apply to be granted such a warrant - all LEA persons, such as the RUC Chief Constable[14], and the Commissioners of Customs & Excise[15]. The LEA desire that a target be personally the subject of an interception warrant rather than a specific address is facilitated under RIP Act section 8(1).[16]

A warrant may be issued by the Secretary of State, inter alia,

"(a) in the interests of national security;

(b) for the purposes of preventing or detecting serious crime;

(c) for the purposes of safeguarding the economic well-being of the United Kingdom..."

Broadly the same conditions stand for the obtaining of a court order authorising an interception in the USA: see, for example, 18 USC et seq., as amended by the Electronic Communications Privacy Act 1986, under which only an LEA may require a telecommunication carrier to undertake an interception, and only when such has provided or may provide evidence of a federal felony. Further, any interception warrant granted under CALEA will only be authorised by the court if it is a last resort and where it is reasonable - in terms of cost - to expect the relevant telecommunications carrier to comply. In particular, under section 108, a court order enforcing section 103 cannot require a telecommunications carrier to perform an interception and acquisition of call-identifying information (see below) in excess of the capacity for which the Attorney General has agreed that the carrier should be reimbursed.

5. Communications Data & "Call Identifying Information"

Investigatory authorities often wish to access more than just the intercepted data. Associated `communications data', such as itemised telephone bills or a `real world' identity corresponding to a particular internet identity is often sought. CSPs are generally in favour of legal provisions which put this on a clear, mandatory footing, rather than a voluntary system where moral pressure may be brought to bear to disclose information, and the extent of any right to refuse is unclear. However, they also desire that the exact nature and extent of information does not exceed that which they may have agreed to hand over before. Some opinion exists which would suggest that there should be an obligation to provide a legible printout of requested data, the justification for such a requirement being that it is less intrusive than a search and seizure order which could be used to take company hard disks, for example. The UK Data Protection Registrar has recognised that while communications data hand-overs remain voluntary, CSPs are placed "under considerable moral pressure to co-operate with the police."

The US debate is comparable to that in the UK. The hand-over of communications data extraneous to the content of an intercepted communication is to some degree a requirement of CALEA. Section 103 (2) obliges the telecommunications carrier to hand over "call-identifying information" which is reasonably accessible either before, during or after transmission of the telecommunication or at a later point in time which may be set by government, in a form which permits association with the content of that message. "Call identifying information" is defined as[17]:

"dialling or signalling 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 telecommunication carrier."

The debate over the above list of capabilities as proposed by LEAs has centred on interpretation of what is and is not covered by this section.

CALEA is explicitly functional rather than technical in what it requires of telecommunications carriers (see section 103 (b)). However, the debate over feasibility of the act in practice has proven to be inescapably bound up with technology. For instance, the FCC Order permits the obtaining, without a warrant, of some `post-cut-through' content, which can be entered using a touch-tone telephone during the course of a call. The difficulty arises in relation to distinguishing between dialled digits which are clearly call-identifying, such as further digits dialled in a telephone number after the subject has connected to a long distance provider[18], and those which are clearly content, such as a bank account number.[19] Where such fine technical distinctions exist, it can be difficult to isolate what information falls into which category - particularly important if a warrant is required for one and not the other. It is difficulties such as this that both the industry and privacy-rights activists emphasise when arguing that the system provided for under CALEA's authority is unfeasible in practice. In August 2000, a District Court of Appeals in the US ruled that where such information is required in circumstances that call-identifying information is not separated from content, the investigating authority will require a content-level warrant in order to be able to demand its handover.[20] It remains to be seen whether the UK will follow suit or find some alternative way of dealing with such ambiguous situations.

Under the RIP Bill, the analogous term is `communications data', was defined to include "any address or other data comprised in or attached to a communication..." as well as "any information...that is held or obtained, in relation to [the relevant] persons..."[21]

This definition was overly broad. For example, a third-party systems provider may hold all the personnel files on a particular employee of the customer, as part of an outsourcing arrangement, which would potentially have been accessible under these provisions.

After much heated debate between government, industry, and privacy rights interest groups, this section was redrafted. Section 21 (4) of the RIP Act as it now is refers "any traffic data" Further clarification is to be provided by the introduction of a Code of Practice for the Interception of Communications Data and Accessing Communications Data. A draft code was released for public consultation between September and November 2000; the results of this process have yet to be released. This is a welcome step providing that it does indeed help to streamline the process rather than add an extra layer of bureaucratic requirements.

6. Encryption

Lastly, an area of much concern is that of encryption. Various controversial suggestions have been made by investigatory authorities keen to have the power to require that intercepted data be provided in an intelligible form, most particularly that this be facilitated by the mandatory hand-over of encryption keys with which to decipher encoded information. As encryption programs become more widely available this will become an increasingly important aspect of the interception debate. There is even some opinion which would suggest that within the foreseeable future encryption capabilities will render any requirement that CSPs provide interception facilities an outmoded provision: Demon internet, in expounding this view, suggests that this could happen in as little as five years' time. Of course it is for this reason that investigating authorities are keen to acquire the power to demand that encryption keys be disclosed. For example, the UK Regulation of Investigatory Powers Bill, as originally introduced to Parliament, would have granted such a power to those appropriately authorised to, under certain conditions, require that an encryption key be handed over: this could be done under Section 46 on condition that it was necessary either in the interest of national security, or for purposes of crime prevention and detection, or in the interests of the economic wellbeing of the UK, or that (inter alia) the requirement of the encryption key is proportional to the believed benefit of imposing such a demand and only an order under this provision will reasonably suffice to obtain it. The grant of such a power to investigatory authorities was much opposed by the CSP industry in the UK (indeed due to its controversial nature similar provision was removed from the 1999 Electronic Communications Bill). Opponents of this power argued that it represented a

disproportionate breach of privacy and gave wider powers than are necessary or desirable to investigating authorities. It was however mitigated by section 47, which provided that the recipient of such an order may instead elect to provide an intelligible copy of the information sought.

After much debate, the system introduced in the final RIP Act as passed took a much more pragmatic approach. Under section 49, those appropriately authorised are empowered to require "disclosure...in respect of any protected information." As a matter of course the *information* which is necessary to the investigation is to be requested first; only in cases where handover of the encryption key itself is considered to be absolutely essential to the investigation (section 51(4)) should that be requested in the order. That group of persons entitled to request an order for the handover of decryption keys (as opposed simply to the protected information in an intelligible form) is also more limited (section 51 (2)).

As regards the US position, the issue of encryption in only mentioned in one short subsection in CALEA:

"A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication." (Section 103(b)(3)).

Attempts to introduce legal regulation of encryption in the USA have in the past attracted considerable opposition from the privacy-rights lobby[22], which argues that citizens' use of encryption technologies should be completely unfettered. This provision in CALEA is, of course, not considered acceptable by such a mindset, however, it would seem a common-sense measure. An investigating LEA will clearly have no use for encrypted data which is unintelligible without being decrypted - if LEAs have no access to decryption technology, then criminal interests can pass information unhindered. However, it would be nonsensical to demand that the telecommunications carrier involved in the interception be responsible for decryption in every case. (Similar provision is made in the UK Regulation of Investigatory Powers Act, Section 49(1) - although more by implication and default than the clear expression given in CALEA). Of course, in large part the debate over such encryption issues may yet prove to be something of a red herring: it will not be an issue for the many CSPs who do not hold encryption keys for their subscribers.

7. Conclusions

The regime in place in relation to the interception of electronic communications in the USA, and that currently under discussion for the UK, might, as can be seen from the above discussion, be regarded as being broadly similar. That being the case, the UK would do well to give due consideration to the practical application of CALEA in the US. Indeed, the major objections raised to the RIP Act as presently stands by those in the communication service provider industry in the UK - in particular the uncertainty as to any minimum standard of interceptions capacity and the costs to be met - broadly reflect the problems which have been encountered by the US legal system in seeking to practically deploy CALEA. While the non-technical approach which both regimes have adopted is essential in order to ensure that the laws remain `future-proof', there remains a distinct lack of clarity which at least secondary legislation must be drawn up to address. This clarity is essential to the likely success of any such legislation, however, the difficulty in achieving the same is only too apparent in the very fact that although passed as long ago as 1994, CALEA has yet to be fully implemented due to such problems as a failure thus far to agree with the industry a reasonable minimum standard for interceptions capacity, or even the exact balance of costs between the state and business. Those responsible for the passage and enforcement of the RIP Act must ensure that it is effectively operated in practice, or risk creating a monster.

---

[1] See http://www4.law.cornell.edu/uscode/18/ch119.html

[2] "Implementation of the Communications assistance for Law Enforcement Act by the Federal Bureau of Investigation" Audit Report 98-13, 3/98 http://www.usdoj.gov/oig/au9813/a9813.htm

[3] The definitions set out in CALEA section 102 are sufficiently wide to incorporate CSPs involved in the provision of electronic communications, such as email / internet communications, mobile telephony, etc.

[4] See below, *5. Communications Data & "Call Identifying Information"*

[5] Quoted from BT's response to the consultation exercise which preceded introduction of the original RIP Bill, available via the Home Office website http://www.homeoffice.gov.uk

[6] In December 2000, the Home Office initiated a consultation process on relation to the composition of the Section 12 Order. This consultation is set to run until mid 2001. The discussion document offers little in the way of increased clarity.

[7] See below, *5. Communications Data and Call-Identifying Information*

[8] See below, *5. Communications Data & "Call Identifying Information"*

[9]*US States Telecom Association, et al -v- Federal Communications Commission and United States of America* US Court of Appeals for the District of Columbia Circuit No.99-1442; See also below

5. Communications Data & "Call Identifying Information"

[10] IETF "Policy on Wiretapping" http://search.ietf.org/internet-drafts/draft-iab-raven-01.txt

[11] Section 14

[12] Section 109(a)

[13] Under section 109(b)(1)

[14] (section 6(2)(f))

[15] (section 6(2)(h))

[16] "An interception warrant must name or describe either -

(a) one person as the interception subject; or

(b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place."

[17] section 102(2)

[18] See FCC Third Report & Order, para 112

[19] See FCC Third Report & Order, para 119

[20]*US States Telecom Association, et al -v- Federal Communications Commission and United*

States of America US Court of Appeals for the District of Columbia Circuit No.99-1442

[21] Section 20(4)

[22] See, for example, the ACLU's "Big Brother in the Wires: Wiretapping in the Digital Age", March 1998. Available online at http://www.aclu.org/issues/cyber/wiretap_brother.html