THE BRITISH CHAMBERS OF COMMERCE

THE ECONOMIC IMPACT OF THE REGULATION OF INVESTIGATORY POWERS BILL

An independent report prepared for the
British Chambers of Commerce

June 12, 2000

Editors:
Ian Brown, Department of Computer Science, University College London
Simon Davies, Department of Information Systems, The London School of Economics
Gus Hosein, Department of Information Systems, The London School of Economics

Contributors and Reviewers
Ian Angell, Department of Information Systems, The London School of Economics
David Banisar, Electronic Privacy Information Centre, Washington DC
Nicholas Bohm, E-commerce Working Group of the Law Society
Richard Clayton
Mark Drew, Norwich Union
Brian Gladman
Simon Moores, The Research Group
Steve Smithson, Department of Information Systems, The London School of Economics

The British Chambers of Commerce have commissioned this report to assist in the consideration of the commercial issues raised by the Regulation of Investigatory Powers Bill. It has sought to draw on the expertise of a wide variety of individuals acknowledged to be expert in their field. The views expressed are those of the authors and are not necessarily established BCC policy.

THE ECONOMIC IMPACT OF THE REGULATION OF INVESTIGATORY POWERS BILL

EXECUTIVE SUMMARY

General
Business and economic implications
Legal issues
Other key issues

INTRODUCTION

History

About RIP

SECTION A: TECHNICAL COSTS AND LEGAL RISKS

Section A.1: COSTS TO AN INTERCEPTION INFRASTRUCTURE: A very short course in ISP interception

Intercepting in "telco-land"
Intercepting email
Intercepting IP traffic
Where to intercept IP traffic
Routing traffic past the interception point
What IP traffic should be intercepted ?
What costs did the Smith Report forget ?
Who should pay for interception ?

Section A.2 TECHNICAL RISKS LEADING TO BUSINESS COSTS

Security Risks Created by RIP Legislation
Cryptographic Keys
UK-based Internet Service Provision
Business Risks Created by Possible Key Seizure
The Taxpayer Costs
The Additional Costs for Handling Government Classified Information
ISP Interception Costs
- Staff Costs
- ISP Located Interception Equipment Costs
- ISP Accommodation Costs
- GTAC Interface Costs
- GTAC Secure Network Costs
- Overall Interception Costs

The Costs of Key Seizure

Section A.3 TRUST IMPLICATIONS OF KEY DISCLOSURE

SECTION B: BUSINESS AND ECONOMIC IMPLICATIONS

Applicability of RIP
Warrants & Tipping Off
RIPs Role in Forcing UK Commercial Activities Off-Shore
Further Legal Instability : Rip And The European Convention On Human Rights
Interception Costs
The Core Problem : Home Office Incompatibility With Commerce

SUMMARY OF KEY BUSINESS IMPLICATIONS

ASSESSMENT OF ECONOMIC COST

DIRECT COST TO ISPs
COSTS ARISING FROM TECHNICAL DESIGN REQUIREMENTS
OTHER DIRECT COSTS TO BUSINESS
EROSION OF THE UK SHARE IN THE GLOBAL E-COMMERCE MARKET

SECTION C: FURTHER ANALYSIS AND IMPLICATIONS

Section C.1 INTERNATIONAL DIMENSIONS

C.1.1 International Survey on Lawful Access And Forced Disclosure Of Encryption
The Right Against Self-incrimination
C.1.2 SORM: From Russia With Lessons
SORM: Costs and Market Effects
SORM: International lessons taught, lessons learned
International Conclusions

Section C.2 TECHNICAL INFEASIBILITY

Communications
Stored data
Procedural difficulties
The high cost of countermeasures

IMPLICATIONS AND CONCLUSIONS

EXECUTIVE SUMMARY

General

1. There exists a clear need for a rigorous framework for the regulation of law enforcement access to communications media, including the Internet. Placing such regulation within the framework of the European Convention on Human Rights is a welcome and necessary objective. Business requires confidence that efficient and effective policing of criminal activities is regulated by clear and well reasoned legislation.

2. The RIP Bill as it stands is entirely inadequate as a mechanism to achieve efficient and reasonable interception and surveillance Its effect is likely to be loss of confidence in e-commerce, unacceptable costs to business and to the UK economy, confusion and uncertainty at numerous levels of business activity, and an onerous imposition on the rights of individuals.

3. The justification for the Bill has been established to a large extent on anecdote and rhetoric. While attempting to achieve a long term infrastructure for interception and surveillance, the government has failed to produce a threat model to form the foundation for a rational assessment of the need for many of the provisions of RIP.

4. The effect of the Part I provisions of the Bill can justifiably be described as mass surveillance of internet activities without judicial warrant or adequate oversight. The Bill substantially increases the power of public authorities without correspondingly increasing the scope for oversight and accountability.

Business and economic implications

5. The construction of the definitions used in the Bill tends to be excessively broad, leading to substantial doubt as to the level of exposure to cost, risk and disruption for business. Of even greater concern, are the implications that arise as various Agencies explore how this new framework might be 'stretched' in the future. These imponderables cast uncertainty over future investment decisions.

6. The Bill will create significant economic repercussions. It imperils the government's intention of making Britain the most desirable place to trade electronically. As it stands, RIP is likely to create a legal environment which will inhibit investment, impede the evolution of e-commerce, impose direct and indirect costs on business and the consumer, diminish overall trust in e-commerce, disrupt business-to-business relationships, place UK companies at a competitive disadvantage, and create a range of legal uncertainties which will place a growing number of businesses in a precarious position.

7. There is compelling evidence that the enactment of RIP will create a trend amongst UK firms to establish a range of operations offshore, while creating an environment hostile to the creation of, and investment in, new business activities in the UK.

8. The government has substantially underestimated the cost of compliance by ISPs. The most realistic estimate is of the order of £640 million over the next five years.

9. The overall financial implication of RIP, in terms both of losses and leakage from the UK economy, and of cost of implementation, may be in the order of £46 billion in the first five years of operation.

10. The Bill will impose Government-mandated design and technical requirements for communications systems which will have the effect of "freezing" technological advancement thereby discouraging industry from investing in otherwise promising products and services. Government-mandated design and technical requirements would make consumers and industry dependent upon the Government to revise the requirements frequently enough to keep up with technological changes.

11. The practical operation of Section 46 presents a real threat to the security of corporate signature keys, and must be regarded as a major impediment to the establishment of public confidence in electronic commerce in the United Kingdom.

Legal issues

12. There are substantial grounds for the view that the Bill contravenes and compromises a number of legal rights and responsibilities. On the balance of legal opinion, Part III contravenes the European Convention on Human Rights. Elements of part I may breach the Data Protection Act, while the execution of the Bill's provisions in both part I and III are likely to compromise a range of conditions relating to duty of care.

13. The practical implications of RIP will depend to a great extent on the provisions in secondary legislation, and the scope of the anticipated Code of Practice. The fact that the government has failed to provide details of either has placed UK business at a great disadvantage in assessing the legislation.

14. The Bill poses a number of unresolved questions about the position of the legislation with regard to both employment and company law. Amongst the most prominent of these is a potential issue of the Government being deemed to be acting as a 'shadow director'. This raises a number of obvious questions with regard to the potential civil liability of the company if the surrendered keys were used in such a way that an innocent third party suffered loss.

15. It is unclear where the boundary is drawn between 'content' of messages or transactions, (where warranted access is required) and 'communications data' (where access would not appear to require a warrant. The amendments tabled by Lord Bassam to Clause 2 and Clause 20 make this concern even greater.

16. The Bill is unclear about which officials, at what level, in which Departments may seek access to encryption key material and communications data. Of greater importance is the lack of clarity in the Bill on the question of warrant procedure and validation

17. There is considerable concern in the business community on the degree of individual and corporate liability flowing from exposure in other jurisdictions to actions potentially required in the UK to comply with the RIP Bill. If full decryption (as opposed to the generally preferred option of session) keys are demanded using a Section 46 notice with an associated 'tipping-off' order, individuals working for multi-national companies may be placed in a perilous position. They may have compromised the international transactional security of

that organisation yet be directly barred from informing senior management of that exposure. Such an individual may possibly be protected under UK law for these actions but their exposure in other jurisdictions - particularly that of a non-UK parent company – is uncertain.

Other key issues

18. Both Part I and Part III of the Bill raise important questions both for the functioning of media and for the status of legal professional privilege

19. The Part III issue of the reverse burden of proof regarding lost or missing keys carries with it important considerations for civil rights. These provisions also have important repercussions for business for the management and retention of revoked keys.

20. An international survey of laws indicates that the provisions of RIP have been rejected in numerous jurisdictions. The closest parallel is the Russian SORM scheme, which pre-dates RIP, and which appears to have a common genesis.

21. There exist a number of technical means of overcoming the intentions of the legislation. The use of these mechanisms, which include new forms of encryption and anonymising services, will circumvent the provisions of the legislation. The pursuit of solutions will have the effect of driving up costs of compliance and creating more onerous impositions on individual rights.

INTRODUCTION AND OVERVIEW

When uncertainty is too high in the market, regulation is intended to induce confidence and to establish a level playing field. The UK Government has attempted to regulate electronic commerce, encryption services, and now methods of operation of Internet Service Providers (ISPs) in such a way that has in fact introduced a greater level of uncertainty. The *Regulation of Investigatory Powers* bill is widely perceived as a threat to the future of economic growth and the security of technological infrastructure within the United Kingdom.

History

The legislation's genesis began in 1996 with initiatives to regulate security through the control of encryption services. The 1997 *Consultation Paper on Licensing of Trusted Third Parties*, triggered a harsh public response, led by civil liberties organisations and supported in consultation responses by industry.

These negative components were retained in the *1998 Secure Electronic Commerce Statement*. In this DTI document, surveillance and electronic commerce were still intertwined in a market-chilling and technology-freezing manner, although the proposals was labelled as being 'voluntary' regulation.[1]

After Select Committees and consultations, the restrictive market and technical regulations on cryptography were weakened, but not removed. In the *1999 Draft Electronic Commerce Bill*, government presented its new *solution*: unprecedented powers to demand encryption keys from individuals, users, and companies.

Following further consultation on these proposals, and an uproar similar to the 1997 response, the government changed its plans in form, but not in content, and in the November 1999 Queen's Speech, the surveillance proposals and the electronic commerce components were separated into two bills: *The Electronic Communications* (which has finally passed) and *The Regulation of Investigatory Powers*. The latter was introduced with even greater powers of surveillance.

About RIP

The Regulation of Investigatory Powers Bill intends to regulate surveillance powers generally, become consistent with the Human Rights Act, and to update interception powers for the Internet. It is an update to new technology and new issues, but not to new sensibilities.

There are five parts to the Bill:

- Part I: On Interception of communications and disclosure of communications data
- Part II: Surveillance and covert human intelligence sources
- Part III: Investigation of electronic data protected by encryption etc.
- Part IV: Scrutiny etc. of investigatory powers and of the functions of the intelligence services
- Part V: Miscellaneous and supplemental

The primary focus of this report, is on parts I and III of RIP as they relate most to the Internet, industry, encryption, and electronic commerce. Parts II and IV are of concern with regard to civil liberties and legal procedures, and although some of these issues will be raised in the analysis of parts I and III, they are generally outside the scope of this study. Further information on civil liberties concerns is provided in great detail on the web page of the *Foundation for Information Policy Research*[2] and through the campaign group *Justice*. Part V will also be raised in our review of parts I and III.

---

[1] Caspar Bowden of the *Foundation for Information Policy Research* (FIPR) refers to the voluntary nature of the regulation as "the use of coercive inducements", in "Unprecendented Safeguards for Unprecedented Capabilities", by Caspar Bowden, presented at the Hoover Institution at Stanford University, National Security Forum Conference, "International Cooperation to Combat Cyber Attacks", December 7, 1999.

[2] The FIPR web site is available at http://www.fipr.org

Of particular concern within Part I, is the *updating* of interception in application for digital telecommunications, particularly the Internet. Warrants for Internet interception will continue to be issued under the Secretary of State, thus are not judicial warrants, and may be provided in a blanket permission. According to the Stand.org analysis:

> In fact, the Security Services have a mandate to monitor all incoming and outgoing international traffic, without regard to who it's from or to, merely under the control of a general permission from the Home Secretary.[3]

Due to the international nature of the internet and its resources, where users have email accounts on servers abroad, they can be monitored by the security services and police with almost no legal oversight. Meanwhile, under a secrecy clause, ISPs are prevented from notifying their users of any interception warrants.

The technical measures required for such surveillance are defined in Part I, section 12. This requires ISPs to develop the technology needed to intercept the communications of their customers. Section 20 requires access to *Communications Data*, which is an ambiguous term[4] defined as:

> any address or other data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;

Applied to the Internet, this involves *a significant increase in surveillance powers*. This level of surveillance includes a listing of all web sites a user has accessed, all (intended) recipients of sent and received emails, and all logon transactions with the ISP including telephone numbers of access. It is more than knowing, in the telephone analogy, the telephone numbers dialled by the user under suspicion: traffic data on the Internet shows all a user's movements on the Internet, and amounts to watching all activities and server visits. Of great concern is that a request for traffic data does **not** require a warrant, and can be given to any government department, under Section 24(1f) in the interests of detecting *any* crime, and not necessarily a *serious crime*, as is required under surveillance warrants.

In practical terms, this requires the development of *black boxes*, installed at each ISP, that will send traffic data to the Government Technical Assistance Centre (GTAC), located within the Security Services. This scenario was developed in a report commissioned to a group of consultants by the Home Office, entitled the *Technical and Cost Issues Associated With Interception of Communications at Certain Communication Service Providers*, hereafter referred to as the Smith Report. The Smith Report places a £30 million price tag on intercepting communications on the Internet. Section A.1 of our report reviews the Smith Report and provides as a critique, a technical review of the associated costs of interception on the Internet, and a study of the impact of Part I of RIP on the UK ISPs.

Part III of RIP is almost a direct transplantation of the most contentious components of the *Draft Electronic Commerce Bill 1999* into RIP access to *encryption* keys. Encryption is the means of securing data by transforming it into an unintelligible form that can only be *decrypted* by the intended viewers, with the use of an encryption key. Strong, unbreakable encryption is an essential requirement for electronic commerce, security, and trust.

Part III allows for the warranted access to encryption keys of individuals, users, and companies for the purpose of *any type* of investigation under any type of statutory requirement (section 46.2), or *any crime* as well as the economic well-being of the United Kingdom (section 46.3). An associated offence is the secrecy clause: a warrant may include the requirement that its existence must not be disclosed. This raises severe liability concerns, even beyond the secrecy constraints of Part I . The implications of this are discussed in Section A.3.

Section B of this report discusses in detail the economic impact of RIP. This section analyses the impacts that RIP will have on business operations. The analysis conclude that the compliance costs to ISPs alone

---

[3] From the Stand Guide to RIP, version 1.0, available at http://www.stand.org.uk/ripnotes/.

[4] Communications Data 'is often more elaborately referred to as *traffic data.*

are likely to be in the order of £640 million in the first five years of RIPs operation. The overall financial implication of RIP, in terms both of losses and leakage from the UK economy, and of cost of implementation, may be in the order of £46 billion in the first five years of operation.

RIP creates another new offence in section 49: a refusal to hand over a key can result in imprisonment for two years. If a key is lost, or the password is forgotten (which occurs frequently), the threat of imprisonment remains. Such a warrant scheme has twice been found under legal audits to be incompatible with the Human Rights Act because it reverses the burden of proof, as the defendant must prove a negative. This is further discussed in Section B, while Section C.1.1 summarises an international survey showing that similar key seizure legislation exists only in Singapore, Malaysia, and as a pending effort in India. Meanwhile other countries, such as Denmark, have decided against pursuing any such policies, and Ireland has recommended against the disclosure of keys. Some countries, such as the US, are in fact legally constrained from imposing such measures.

Section C.1.2 returns to the development of an infrastructure for interception, and discusses how only one other democratic country has developed such an infrastructure: Russia with its *SORM* system. This system is outlined in detail to prove the direct similarities with the UK's RIP, and presents the business costs. This section concludes that internationally, the UK is acting as a test subject for oppressive regimes.

Section C.2 looks at the effectiveness of RIP warrants in the light of developments in security techniques. Even without the impetus provided by the legislation, these are likely to render many of the RIP powers ineffective. This will lead to an expensive surveillance infrastructure with little effect against crime, inevitably causing law enforcement agencies to demand more coercive powers.

.

SECTION A: Technical Costs and Legal Risks

The Bill mandates interception capabilities on the Internet and access to communications/traffic data in such a way that it assumes that the technical infrastructure to provide it is trivial. This is far from the case. As the Smith Report began on the costs and technical considerations, we take this further in section A.1 to show that the technical risks and the business costs are unwieldy, and completely unreasonable for the gains of interception. We will present the technical requirements for intercepting ISP traffic and accessing ISP traffic data, including considerations that the Smith Report omitted to include in its analysis. This will be followed by a discussion of the cost implications to business.

Section A.2 continues along this line, and introduces the notion of risk: both the GTAC and the ISPs will have to bear some risks in managing and maintaining access to traffic data and keys. These risks, we argue, bear a significant cost that the UK Government and the Smith Report have failed to acknowledge.

Continuing with the risks of Part III of the RIP bill, section A.3 investigates the legal implications of access to keys, and the associated corporate liability associated with key disclosure, the trust components that are often misunderstood, if not ignored because of the important details to electronic signatures and cryptographic techniques. We present here an argument that RIP creates an intolerable dilemma within the corporate environment and a destruction of trust, while solutions to this dilemma requires either extraneous costs, a weakening of security, or more time as further technology is developed.

The sum is that RIP is costly, risky, and a detriment to the trust and technical infrastructure that the UK is attempting to create as the backbone to the "best place for electronic commerce in the world". Again, surveillance interests are compromising economic interests, as industry continues to await a favorable regulatory landscape in which to function and prosper.

Section A.1: COSTS TO AN INTERCEPTION INFRASTRUCTURE: A very short course in ISP interception

Intercepting in "telco-land"

People access the Internet in the UK in two main ways. They either dial up an ISP, using a modem or the ISDN equivalent or they have a hard-wired permanent connection (such as a leased line, cable modem or ADSL connection). Less important methods of access include cybercafes and other shared access systems.

If a party wishes to intercept hard-wired connections it makes a lot of sense to do this somewhere near to the person it is targeting. If not, then it is has to sort out the target's traffic from that of other peoples' traffic. This can be expensive. The machinery for doing the interception is also expensive – but if the number being observed is fairly small (perhaps 500 targets per year - 200 at once) then the technical infrastructure is minimal.

If the intercepting party want to intercept dial-up connections it may still find it easiest to do in Telco-land, on the pole outside a house or at the local exchange. However, if your target is moving around from place to place you cannot do this. It may, however, be reasonable to assume that they are using the same ISP all the time (or a small set of ISPs) and so you will wish to intercept them there. Here, our troubles have just begun!

Intercepting email

If the interception aim is modest, just to read the target's email, then the task may be simple. Even with permanent connections and certainly with dial-up accounts, the ISP will be running a store-and-forward system for email. Making a copy of the email as it passes through the ISP system is straightforward – you just need a configuration file that says this is to be done. Such a file can be trivially created by any administrator when served with a suitable warrant.

Unless the intercepting party is unlucky, the target will also be using the ISP's systems for store-and-forward for outgoing email as well. This means that email can be captured in both directions.

Of course, making a copy of the email is only the start of the process. The email needs to have various forensic information added (timestamps, identity of target, place of interception and so forth). It then needs to be securely sent to the Government's GTAC for passing onward to the correct agency who wanted the interception done.

> *The Government sponsored Smith Report calls this email interception process "active interception" and estimates some fairly low costs for it:*
>
> > *for the smallest ISP, £44,700 year one, £19,400 per annum thereafter*
> > *for larger ISPs £113,300 year one, £41,900 per annum thereafter*
>
> *The industry's view appears to be these figures are of the right sort of magnitude for small ISPs and an underestimate for large ISPs.*
>
> *There is an up-front cost for software development of something like £500,000. But the Smith report hints that this software may already exist in part and that it would be advantageous for the Government to supply a standard version to all ISPs since this will allow the use of standard procedures at GTAC.*
>
> *The Smith Report consultants are so keen on "active interception"'s apparent cost-effectiveness that they recommend its universal deployment. This ignores whether this would be value for money (with only 500 targets per annum many small ISPs would never be called upon to intercept anyone) and also ignores the apparently minor matter that many small ISPs could not afford this cost. The Smith report does suggest a split in the costs between ISP and Government which would reduce the first year cost to the ISP to £18,800 (£9,400 in later years) but this is still sufficient to directly impact business plans.*

Intercepting IP traffic

Of course, not all email passes through ISP store-and-forward systems and not all communication is email. In order to intercept all possible communication it is necessary to intercept all Internet Protocol (IP) traffic.

Intercepting IP traffic has a number of important differences from other interception regimes, such as are already in place for the postal system and for telephones.

- *IP networks are not reliable*. This means that traffic can be resent when a failure is seen, which means that data streams must be reconstructed. This is not technically difficult, but adds to the cost and complexity. Since the "real" data being intercepted is just using the IP network as a carrier it is essential to perform this step before any attempt can be made to decipher the higher level protocols to expose the actual "message" to be intercepted.

- *IP networks are "packet switched".* This means that traffic does not necessarily travel the same route. **This means that all possible routes must be intercepted**. The nearer the (unique) end point that you are, the easier this becomes.

- *IP networks are efficient.* This means that data will not flow any further than it needs to. A telephone call to next door will travel via the local exchange, a letter written to next door may well go to the regional sorting office. IP traffic between two dialup users connected to the same "modem" (called a NAS (Network Access System)) at the ISP will never leave the NAS to pass over the ISPs network. The nearer the edges you intercept the less traffic has been "short-circuited" and is therefore invisible to your intercept.

Where to intercept IP traffic

Intercepting traffic in the "middle" of an ISP network looks superficially attractive. There's lots of data flowing there, so surely it must be worth looking at. This isn't so:

- As discussed above, intercepting in the middle of the network means that you will miss traffic that never entered the centre parts of the network.

- As discussed above, you have to intercept all possible routes. A single route means a single point of failure and network designers produce a mesh of connections so that single failures do not impact the network's functionality. There is some truth behind the popular myth that you can nuke New York and the traffic will route around this "failure".

- The most telling reason for avoiding intercepting in the middle of ISP networks is that there is a very large amount of data there and it is flowing very fast indeed. This pushes up the cost of interception for both reasons. You have to filter out the traffic you want to see – and you have to do that filtering in very short time intervals.

So, all the indications are that you should tap at the edges of the network.

Unfortunately there are many edges, which makes this process expensive. An intercepting party cannot, even with modern ISP modem pool designs, predict which edge a dialup customer will be using. Their end of the dialup connection may be fixed, but temporary loading issues may mean that the a series of calls can be delivered to NAS equipment in adjacent rooms or hundreds of miles apart.

So economics drives the process back to the centre, which is equally expensive..

Routing traffic past the interception point

The authors of the Smith report believed they had found a way out of this conundrum. They suggested that it would be possible to route traffic from the edges through a special network path, so that it all went past a single intercept point. This is superficially attractive, but has some rather significant flaws:

- The technology they proposed to do this routing ("policy based routing" and some other schemes) does not actually work in practice. The capability is only present in some equipment, but even then there is massive performance cost of turning it on. Where capability is present, there is the likelihood that the ISP has purchased the equipment to use that capability for other purposes – so it is not "spare" just for interception purposes.

- The special routing creates single points of failure. Since interception moves data over seldom used equipment there is the real likelihood of outages – compensation for which does not figure in the Smith report figures.

- It is extremely complex on real networks to route all traffic past a single point without creating delays or allowing the user to otherwise detect an unusual traffic path. ie: the interception will not be invisible to a cautious user.

To summarise the difficulties: there is a complex trade-off in deciding where to tap – to which there is no simple answer beyond the one started with – tap at just exactly the one place you need to.

What IP traffic should be intercepted ?

So now, one should consider what to tap. In the simple case of email we started with, the email for the target could be readily identified by its address. When you are intercepting at the Internet Protocol layer you need to know which IP address to tap. This is rather tricky because for dialup connections the IP address is usually assigned dynamically as the session starts.

IP addresses can also be assigned dynamically for leased lines as well, using protocols such as DHCP. If one wishes to intercept a single machine within a company then access to the company DHCP machine is needed to know what to target. This may be complex to arrange if you are not prepared to trust the administrators of the DHCP machine, even under the secrecy clause.

For dialup, IP address allocations are usually reported to (or made by) the authentication system as part of the process of checking login credentials such as username and password. The common system for this is called RADIUS though there are other systems in daily use.

The Smith Report suggests two schemes. The first is altering the RADIUS system directly to report IP address assignments (they recognise the most complex aspect of this, that every ISP is running a different version of RADIUS – usually the one that was current the day that they launched their service!). The second scheme in the report is to "sniff" the traffic to and from the RADIUS server and deduce the IP address by seeing it go past.

The report calls the first scheme "semi-active interception" and the second "passive", though these terms are also bound up with the ideas they had for special routing of packets so as to reduce the number of interception points.

> *The Smith report estimates the costs of implementing a passive scheme at a large ISP as £1,384,000 with less than half being the Government's "share".*
>
> *For the semi-active scheme they estimate £217,300.*
>
> *Industry has been less than charitable about these estimates.*
>
> *The semi-active scheme is perceived to be unworkable on large networks. The passive scheme is seen as having underestimated both the costs and the number of places where tapping would have to be done.*

What costs did the Smith Report forget ?

The authors of the Smith Report provide some detailed cost breakdowns, which suggest a comprehensiveness that is not actually present.

As has already been indicated they have not included any costs for the lowered reliability of the more complex systems they propose. They have also failed to include any compensation for outages that would be necessary for the systems to be rebuilt.

Their estimates for the interception points themselves assume low levels of technology. The high speed components that would be needed at the centre of the country's fastest networks cost far more than is suggested. Their estimates of the costs of filtering equipment also assume low traffic levels – again suggesting that their figures may be only be considered reliable for fairly small networks.

The biggest cost that has been omitted is "opportunity cost". There is a significant shortfall of trained staff throughout the industry. If significant numbers are to be planning and building interception systems then they will not be doing productive work. There is no element in the Smith report for missed opportunities in an industry where "first to market" is an extremely common formula for overwhelming success.

Who should pay for interception ?

The part of interception problem that Government seems to find the most complex is in fact the most easy to understand and solve. This is the vexed question of who should pay for it.

The Government has suggested that it should pay the "marginal" per-intercept costs and the ISPs should pay for the infrastructure. The Smith report shows this coming out as about half and half – though if you accept the industries view that their costs have been wildly underestimated, then the proportion they would be paying would be far more.

The ISPs have suggested that the Government should pay for everything, balancing the expenditure on interception against the other calls on the policing budget such as rural crime cars.

The ISPs argument is that a universal obligation will send weaker companies to the wall, which no one wants to see happen. If there is not a universal obligation then the ISPs will not co-operate by volunteering to be intercepted – so the Government will act arbitrarily on the basis of their perception of which ISPs should be forced to install equipment. This will distort the market by favouring ISPs who manage to grow whilst keeping a low profile.

The Government's argument is that by promising to pay for "everything" they are handing the ISPs a blank cheque to build new networks at public expense.

The Government's argument is weak. Unless some way can be found to measure and recompense for "opportunity cost" it will be a poorly focussed ISP that feels that the Government's project is more lucrative than the other opportunities in the marketplace.

Section A.2 TECHNICAL RISKS LEADING TO BUSINESS COSTS

Security Risks Created by RIP Legislation

Companies and organisations that make extensive use of the Internet are increasingly recognising the need for good information security, both for their own safety and for that of their clients and customers. For e-commerce in particular there have been widespread concerns about the vulnerabilities arising from Internet use. These must be overcome if e-commerce is to achieve the success that many hope for and expect.

Cryptography is now universally seen as a critical technology on which e-commerce will depend. It provides the basis for data protection and privacy and is also the key mechanism for identifying the parties to transactions, for authenticating data and for providing the digital signatures that are widely seen as an essential basis for electronic transactions.

RIP is likely to have a serious impact on the ability of businesses located in the UK to use cryptography effectively. Although the provisions in the legislation for access to cryptographic keys are intended to impact on criminals, the major impact will fall on businesses and their clients.

Cryptographic Keys

When businesses use cryptography to protect information exchanges with other businesses or with their clients and customers it is essential that the keys they use should be well protected: anyone who can obtain copies will be able to access the information that they protect. Many types of cryptographic keys should never be shared with external organisations and must remain under the sole control of a small number of highly trusted company staff at all times. Some cryptographic keys may need to be shared with other businesses to allow secure information exchanges: where this is necessary it is essential that all parties who have copies of the shared keys apply the same standards of key protection. Shared information will be vulnerable if one party is not adequately protecting their keys.

If the keys being used to protect critical business information are revealed to an outside party who might not adequately protect them, the protected information may become vulnerable. In particular, if keys that do not need to be shared are revealed to others, the business information being protected may become vulnerable because the business no longer has sole control of them. Maintaining the secrecy and sole control of such keys is hence vital for effective security, but is a task that the RIP legislation undermines.

The UK government is acutely aware of the difficulties that seizing keys will pose for businesses and has in consequence made a considerable effort to meet such concerns. In particular the Home Office has said that RIP legislation will only allow keys to be seized in 'special circumstances'. Unfortunately, no details have been given of the sort of circumstances that the government has in mind and this means that the risk of key seizure cannot yet be quantified.

Where a security risk can be quantified, a business decision can be made on whether the level of risk is tolerable or whether steps need to be taken to counter it. But when such a risk is of unknown extent, security decisions have to err on the side of caution by planning on the assumption that it is a much larger risk than it may turn out to be.

The impact of such risks on business decisions is most easily illustrated by considering the scenario of a UK company co-operating within an international consortium bidding for a very large contract in competition with other parties. Bid planning would need to be conducted in conditions of utmost security where good cryptographic protection is essential. Procedures must be in place to protect keys and limit any damage caused by their compromise. RIP causes problems for both. More than 30 government authorities have the authority to requisition keys, and secrecy orders can prevent the dissemination of information needed to assess any impact of compromise on the security of bid or business information. Under these circumstances, a consortium may be unwilling to include a UK partner because of the risks caused to the rest of the group.

Security risks that cannot be fully quantified can have a severe impact on both security and business decisions. Good security depends on establishing a very high degree of trust and confidence between

those involved and even small uncertainties about security risks can have a big impact on business decisions. Security decisions have to be highly conservative and this requires that even small risks have to be removed if at all possible. In consequence, while the risk of key seizure by government authorities in the UK might be thought to be small, it will almost certainly have a disproportionate impact on the trust and confidence that overseas companies have in dealing with their UK counterparts. In consequence UK companies are likely to be seen in a less favourable light as potential business partners.

UK-based Internet Service Provision

As the Internet has matured there has been a progressive specialisation and differentiation of many of the services that are involved:

E-Commerce Site Hosting	third party provision of e-commerce sites
Web and Email Hosting & Forwarding	third party provision of (small) company domains
Internet Service Provider	basic Internet access (web, email)
Telecommunications Service Provider	basic communications service provision

The lowest layer in this hierarchy - telecommunications - is now fairly mature (although highly dynamic) but significant changes are underway in the higher layers. The advent of the 'free ISPs' for consumers and home users has forced the more established ISPs to move upmarket and concentrate on support for business and professional use. This has shifted focus to better levels of service reliability and to services such as the third party hosting company web sites and the provision of company sites offering web-based purchasing of consumer goods and services.

The development of services for hosting company e-commerce sites is likely to be a significant factor in the development of e-commerce for small companies and businesses since such organisations are unlikely to have the expertise needed to set up and operate e-commerce web sites on their own.

Third party hosting is also important for consumers because the prospect of many small companies with little or no security expertise setting up for on-line trading is unlikely to provide consumer confidence in the safety and security of such sites. It is worth noting that there have already been several embarrassing examples of web commerce site security failures involving large companies, so it is unrealistic to expect that small companies could avoid such problems without substantial external support. Hosting services are hence likely to be very important in the evolution of e-commerce for small and medium sized businesses.

Unfortunately the RIP legislation is likely to have a detrimental impact on UK-based companies that offer such services. Any company that is considering the hosting of its company web site will want very good security guarantees about the security of the operations that will be conducted on its behalf. Site hosting companies will have many clients and the operations conducted for each client have to be rigorously separated. This is an area where cryptography is likely to be heavily used and a hosting company will not only have to manage its own keys but also the keys of many of its clients. This is an enormous security challenge in its own right but the addition of a requirement that all such keys might have to be supplied to UK government authorities could easy turn a difficult job into an impossible one.

E-commerce site hosting companies will have their own cryptographic keys, which, if subject to seizure, might pose security risks for every one of their clients. If seized, the resulting need to revoke the key would be likely to have a significant 'ripple down' impact on all of the e-commerce sites that are being hosted. There will be procedures and mechanisms in place to handle this but emergency revocation and the installation of new keys is not an easy or risk free exercise.

Worse still, any compromise of such a key while in government hands would put all of their clients at risk and while the chance of this may be small, the consequences if it happens could clearly be very severe. Moreover, the hosting company would have to take the blame since they could not tell their clients that the government had compromised the key. And there are no provisions for compensation from the government if this happens so they would carry this risk on their own.

If a client key is seized there are many issues and uncertainties. The secrecy clause, or 'tipping off' offence would prevent notification of the client whose security might be at increased risk. The client could be encouraged to revoke their keys but no client would do this without seeking an explanation of why this was necessary and such information could not be supplied. In any event a client considering third party hosting of their e-commerce site who is serious about site security will almost certainly wish to impose contractual terms prohibiting the revelation of keys to parties and no UK-based site hosting company could accept such a contract.

UK companies already face stiff competition from overseas hosting companies but RIP will give their competitors major advantages. Hosting companies based in countries such as Germany and Ireland, where the governments are strongly opposed to legislation that gives access to keys, will be able to guarantee that keys will be under the control of the hosting company at all times, a security guarantee that UK companies could not give as a result of the RIP legislation.

The provisions for access to keys in the RIP legislation are hence likely to put UK hosting companies at a disadvantage when compared with their counterparts in other countries. This is not only likely to drive such business abroad but is also likely to have a detrimental impact on small business e-commerce development in the UK. This conflicts in a very direct way with the Government's stated aim of making the UK a 'world class' e-commerce location.

Business Risks Created by Possible Key Seizure

The above examples illustrate that the possibility of key seizure by UK government authorities leads to a number of potential business risks for UK based companies and businesses:

Public Disclosure of Critical Company Information

The accidental or deliberate disclosure of a seized key while in the hands of government authorities could result in the public disclosure of critical business information.

Increased Opportunities for Industrial Espionage

If government authorities do not protect keys to the same standards as the key owner, it will be easier for a competitor to obtain access to trade secrets by penetrating government protection rather than that companies themselves employ.

Reduced Trust and Confidence in Company Security

Overseas companies considering initiatives that might involve UK companies may view the latter less favourably because they see that such co-operation may put any business information that is shared at increased risk.

Because of this they will be less inclined to co-operate with UK based companies and less inclined to share their critical information with them. UK companies will hence be seen as less attractive partners in international joint ventures where information security is an important requirement.

Market Disadvantage

UK based companies offering services where information security is important - for example, e-commerce site hosting - will be at a disadvantage when competing with companies in other countries where government access to keys has not been imposed.

Customer and Client Concerns

Customers and clients, especially those based outside the UK, will be sensitive to the possibility that the UK government might have access to the information that they exchange with UK-based Internet companies and this may reduce their confidence in their safety, security and privacy when using UK-based Internet services.

The Taxpayer Costs

It is very difficult to provide an accurate estimate of the cost to the taxpayer of the measures in RIP because the government has provided very little information on the facilities that they envisage.

Moreover, since there is a considerable debate between industry and government on where these costs should fall, it makes more sense to consider overall costs before considering where these costs are most likely to fall.

In considering the technical costs involved in implementing the provisions of RIP two related elements have to be considered: the interception of Internet traffic and key seizure.

The Additional Costs for Handling Government Classified Information

A number of areas can be identified where additional costs will be involved because ISPs will be involved in the handling of government information classified at SECRET. These are as follows:

- **Staff Costs.** The costs of clearing and training ISP staff in the handling of Government classified information;
- **ISP Located Equipment Costs.** The additional costs of purchasing computer and network equipment capable of processing data that has a government classification of SECRET;
- **ISP Accommodation Costs.** The costs of physically housing such equipment and protecting it from tampering and interference;
- **GTAC Interface Costs.** The costs of providing high-grade firewalls that are capable of connecting systems processing SECRET information to the Internet.
- **GTAC Secure Network Costs.** The cost of the secure network required to connect between equipment located at many ISP sites and the GTAC site in London.

ISP Interception Costs

An outline of the possible interception approaches has already been provided to the Home Office in the Smith report. This identifies the likely initial and ongoing annual costs for both ISPs and taxpayers for three different options:

- Active Interception - the interception of electronic mail
- Semi-Active Interception - interception of IP traffic but relying on support from ISP systems
- Passive Interception - interception at IP traffic but without ISP system support.

In order to simplify the analysis here it will be assumed that the interception regime involves 20 large ISPs and 100 small ones. Moreover, annual costs will be assessed on the basis that the initial costs identified by the Smith Report will most likely have to be reinvested periodically to cope with ISP network evolution. A three-year reinvestment cycle will be assumed. On this basis the total costs using Smith's estimates range from £3,500,000 to £12,000,000 per annum depending on which option is selected.

But these cost estimates are too low because they do not take into account the fact that information on the targets for interception is classified information at the SECRET level and hence requires special handling using appropriate government security procedures. The estimates provided are based on the use of commercial equipment that is not suitable for handling government classified data and this has led to much lower cost estimates than are likely to be achievable in practice.

Staff Costs

The Smith Report's passive interception option involves the smallest staff costs since only the interception boxes at ISPs have access to SECRET data and these may not need to be managed by ISP staff. In the remaining two options, however, ISP staff are required to assist in the process of identifying and routing target traffic to interception points and this will mean that system administrators will have access to government data classified at SECRET and will all have to be appropriately cleared.

For small ISPs only a small number of staff will be involved but it would be impossible to reduce this number below two. For large ISPs many staff are likely to be involved in system administration although it might be possible to clear only a subset of them. Using a figure of 10 staff for each large ISP and 2 for each small one suggests that 300 staff in total could have knowledge of interception targets. And assuming that staff change every three years, 100 new staff each year would have to be cleared and trained in the handling of Government classified material. Using an estimate of £2000 per clearance, £1000 for staff training and costing 10% of staff salaries against such duties, the resulting overall costs would be of the order of £500,000 per annum.

ISP Located Interception Equipment Costs

The main difference here would be the need to replace commercial equipment with equipment designed to meet government standards for the handling of SECRET information. In the past the costs have been a factor of as much as 10 higher but in order not to overestimate the costs a much lower multiplier of 3 will be used (this is certainly much lower than experience of MOD secure systems purchases would suggest). This would increase the earlier estimates derived from the Home Office analysis to give costs in the range from £10,500,000 to £36,000,000 per annum depending on interception option. In practice, however, the passive interception option might be implemented on lower cost commercial equipment because it does not need to separate target traffic from other data so the cost overhead here is likely to be much less. Hence the equipment cost range is more likely to be £10,500,000 to £16,000,000 depending on option.

ISP Accommodation Costs

ISP premises will not normally be capable of offering the physical protection required for handling SECRET information. Such equipment will certainly have to be behind locked doors that offer substantial physical protection and intrusion detection. Moreover, cryptographic equipment will need to be installed and managed and this will bring with it a need for even stricter physical security provisions. While some larger ISPs will already operate from fairly secure premises, it is most unlikely that small ISPs will do so and this will mean that physically secure equipment bays or rooms will be required. This is likely to need a significant amount of additional floor space and could be very costly to provide in prestige locations.

The interception equipment at ISPs will have to be located in close proximity to the ISPs' own equipment racks and this will mean that there is a high risk of data leaking from one to the other via electromagnetic radiation. This risk is well understood within the defence community, where the techniques needed to suppress or prevent such emissions have been developed over many years. The techniques involved are almost unknown in commercial equipment and this means that either high cost equipment designed for defence use will have to be purchased or commercial equipment will have to be housed in screened rooms to prevent electromagnetic emissions. In either case the costs will be very high.

The accommodation costs involved in some large ISP locations will be very high. In locations such as Telehouse in London the enormous growth in both the number of ISPs and the physical size of their network and computer systems is already placing a huge strain on the available space with the result that any equipment space is at a high premium. If government interception requirements add to the volume of equipment involved, ISPs are certain to face severe difficulties in locations such as this where space is not available. It may hence be necessary for an ISP to reconfigure its existing systems to accommodate this additional equipment.

The costs involved in building and housing equipment capable of handling SECRET information is difficult to estimate without a precise knowledge of the character and physical location of all the ISPs involved. However a reasonable estimate of these costs would be £5000 per annum for a small ISP and £50,000 per annum for a large ISP. Using the earlier ISP numbers this results in costs of £1,000,000 per annum.

GTAC Interface Costs

The technology to safely connect systems containing SECRET information to the Internet does not exist and this is recognised in government regulations for handling SECRET data, which do not allow such connections. Given this situation it is far from obvious how interception systems that contain SECRET information about the targets of interception could ever be connected to the Internet but this appears to be what the Home Office intends to do.

Since it is not currently feasible to meet this requirement it must be assumed that the Home Office intends to carry the risks involved in such connections. The Smith report does include network firewalls at a number of critical points in the interface between ISP and the GTAC delivery network but it seems most unlikely that the cost and risk issues of handling SECRET information on the GTAC side of such interfaces have been fully assessed. But the additional costs involved have not been estimated here because there is no sound basis on which to do this given that the required technology is not available.

GTAC Secure Network Costs

The Home Office cost estimates do not appear to include the costs of the secure network required to connect between ISP locations and the GTAC site in central London. The costs of such a network would be very high if it were to be dedicated to GTAC use but it seems more likely that an existing or planned government secure network will be used to meet this need. This will greatly reduce interception costs since this programme will only have to bear a small part of the total cost.

But it is not quite this simple. For GTAC to use existing or planned government secure networks will require that these networks include all ISP locations, a new requirement that will have significant cost and security implications for the network or networks in question. If GTAC traffic and other government traffic flows on a common network that includes many non-government nodes at ISP sites, the vulnerability and risk assessment for the network will change radically. Such consideration will increase the cost of the network for other users and these additional costs would need to be attributed to the interception requirement. Even in a shared network situation the costs are hence likely to be very significant.

An idea of the costs involved in wide area secure networks can be gained by looking at MOD experience where costs are several hundreds of millions of pounds for implementation and several tens of millions of pounds for annual running costs. However these networks support very high bandwidths and, more importantly, are designed to survive a full scale attack on the UK. The cost figures would be a great deal higher than those for a secure network to support GTAC.

But operating a national network capable of handling secret data will not be cheap and the interception requirements will need to bear their share of such costs. These costs seem most likely to be in the one-ten million pounds per annum range based on the ISP numbers used earlier.

Overall Interception Costs

When these costs are combined using the assumptions given earlier the costs of interception range between about £12,000,000 and £18,000,000 per annum depending on the option adopted. These figures do not include the secure delivery network that will be discussed further later. These cost estimates are a great deal higher than those provided in the Smith report because of the additional costs involved in handling SECRET information.

The Costs of Key Seizure

Very little is known about Government plans for handling seized cryptographic keys and this makes it very difficult to estimate costs. But there are some clues as follows:

- Keys will be held (and presumably used) at the GTAC facility in central London.
- But keys may have to be seized at any location within the UK.

- Keys will be needed only in 'special circumstances' and the Home Office have suggested that they are thinking of 'life or death' situations; they have also mentioned the need for rapid response (even down to minutes).
- The organisations that need the decrypted output are spread widely across the UK

These requirements, especially the need for speed, suggest strongly that keys will have to be converted into electronic form local to the point of seizure so that they can be transmitted to GTAC for use since relying on physical delivery to GTAC will be slow. But the costs of supporting possibly many local key conversion facilities would be very high so it is difficult to see how speed of response could be achieved in this way. On the other hand if keys are seized in the expectation of decrypting future messages then the penalty for physically taking the key to GTAC is not a problem. In any event some keys will not be convertible into electronic form and would require physical delivery. So it seems most likely that the intention is to operate in this way.

It is unclear whether it will be GTAC staff that will actually travel and conduct key seizures or staff of the various authorities with the powers to seize keys. The costs of training can be reduced greatly by limiting the number of staff involved but using a centrally located team would greatly reduce the timeliness with which key seizure could be conducted. Many authorities will have the power to seize keys under RIP legislation and if some of their staff need to be able to properly handle keys it seems likely that as many as 500 staff in total may be involved. Cryptographic key handling is a specialist job and requires special clearances and training and when the costs of security clearance, training courses and staff time are taken into account the annual cost of maintaining a key handling specialist would be of the order of £10,000. The staff cost for 500 such officers would hence be £5,000,000 per annum.

Once keys are physically transferred to GTAC for storage and use, the decrypted results then need to be passed back to the agencies that issued the warrants. From the Home Office emphasis on timeliness of product, it seems unavoidable that this will need to be undertaken electronically. Since GTAC will also handle unencrypted intercept products from ISPs, there will need to be a secure distributed computer system to provide a mechanism for distributing results back to the agency clients of GTAC.

These products are highly classified and this means that the computer and network systems involved have to be capable of handling SECRET material. Since nationwide authorities such as the regional Police Forces, Customs and Excise, the Inland Revenue and numerous other government authorities are involved, they will each need computer terminals at a number of locations. Given the number of authorities and their geographic spread it appears that a nationwide system with as many as 500 terminals will be involved. And all of these terminals will need to be connected to GTAC using a network that is protected using high-grade cryptographic capabilities. Moreover, the cryptographic equipment requirement and the classification of the information involved will dictate that all elements of the system have to be capable of handling at least SECRET material and will hence need to be in physically protected locations.

The system software will also have to be custom designed because it will have to meet stringent requirements in terms of correctness of operation, identification and authentication of users and high assurance logging and auditing of all individual transactions as well as meeting requirements for independent scrutiny to ensure that its capabilities are not being abused.

Experience of Ministry of Defence systems of a similar nature suggests that implementation costs for such a system will be in the £100,000,000 to £200,000,000 range. And since computer and network systems age quickly, these costs will recur regularly every five years or so. Operating and support costs over a five year period are likely to double the cost so taking the lower figure would give a five year cost of £200,000,000 or an annual cost of £40,000,000. When GTAC costs are added we can expect the overall taxpayer cost to be of the order of £50,000,000 per annum.

This figure is, however, totally dependent on the assumptions that have been made. Especially large costs are associated with the deployment of secure distributed system for the delivery of results to GTAC clients and the overall cost figures depend heavily on the assumption that 500 terminals would be needed to achieve timely delivery of results to anywhere in the UK where client agencies have a

significant presence. This estimate of the population of terminals is based on the Home Office indication that the rapid availability of decrypted results is a critical factor in their thinking.

Section A.3 TRUST IMPLICATIONS OF KEY DISCLOSURE

Clause 46 of the Bill enables a notice to be served on a person who has had possession of a cryptographic key, requiring either disclosure of the plaintext of encrypted material or (at the option of the person serving the notice) disclosure of the key itself. Failure to comply is an offence, the penalty being up to two years' imprisonment.

Subclause 46(6) of the Bill provides:

> A notice under this section shall not require the disclosure of any key which-
> (a) is intended to be used for the purpose only of generating electronic signatures; and
> (b) has not in fact been used for any other purpose.

This subclause appears to provide a satisfactory protection against compulsory disclosure of signature keys. But its appearance is misleading. The practical operation of clause 46 still presents a real threat to the security of corporate signature keys.

The reason is that all cryptographic signature schemes likely to be deployed in electronic commerce use systems where it is possible to use a key intended for use as a signature key as a decryption key instead (assuming a message has been encrypted by a third party with this use in mind). It is accordingly impossible to say by inspection or technical examination of any particular signature key that it cannot have been used for some other purpose, such as decryption. It therefore becomes a question of fact whether any such key has at any time in the past been used for decryption.

If a notice is served under clause 46 demanding disclosure of a corporate signature key to which a number of corporate users have legitimate access, and the notice allows only a brief time for compliance, the recipient may have no way of knowing or checking whether the key has ever been used for any other purpose than signature. Indeed the notice may prohibit disclosure of the fact that the notice has been served, making it difficult to make the necessary enquiries with any urgency.

Such a case presents the addressee of the notice with an intolerable dilemma. The server of the notice may be assumed to be genuine in the belief that the key has been used for decryption, but is not obliged to provide any evidence whatever to support that belief. There is no mechanism under the Bill for resolving the issue objectively. The addressee must either comply with the notice and disclose the signature key, or refuse and face criminal prosecution. The decision has to be made without any knowledge of the evidence that might show that the key has in fact been used for decryption in the past, and quite possibly without any opportunity to make enquiries about the point. How many system administrators will take the risk and refuse to disclose the key?

It may be argued that corporate systems can be designed with audit trails immediately available to show how a key has been used, and that this will enable certainty to be achieved. Perhaps they can; but will they be deployed, and at what cost? And will system administrators bet their freedom on an audit trail?

It may also be argued that clause 46 notices will be rare, and will even more rarely require disclosure of the key (normally being satisfied with the disclosure of plaintext). Such an argument misses the point: security analysis must start from the question of whether disclosure of a signature key can in practice be compelled. If it can, then the good intentions of government must be weighed against the disaster resulting from the compromise of a signature key.

The effect of such a compromise is that all signatures made by the key cease to be reliable, because it is no longer under the sole control of its owner, and its signatures can no longer be uniquely attributed to that owner. The only exceptions are signatures which can be proved to have been made before the time of the compromise. If secure time-stamping services become widely available, easy to use and widely trusted, the adverse effect of a compromise may be mitigated: but these conditions may take considerable time to be realised.

Section B: BUSINESS AND ECONOMIC IMPLICATIONS

General

The growth of the e-commerce sector relies to a significant extent on the establishment of three conditions:

- a matrix of trust between providers, consumers, investors and government;
- the evolution of efficient, low-cost business structures that are adaptable and responsive, and
- a stable, supportive and efficient legal environment.

The continued prosperity of the sector within any single jurisdiction also requires a sensitivity to the global legal environment. In its broadest sense, this means developing conditions that do not place local companies at a competitive disadvantage to companies in other countries (i.e. a level playing field, or better).

The issue of trust – which underpins dealings between commercial organisations, and between providers and consumers - is predicated to a large extent on a demonstrated commitment to privacy and confidentiality. These factors are crucial in any emerging market, but more-so in the field of electronic commerce.

Commercial organisations surveyed for this report fully recognise and accept the public interest requirement in fighting crime. However, alarm was universally expressed that RIP compromised the core factors that underpin a viable e-commerce sector.

Privacy and confidentiality are central to relationships and contracts with third parties, customers and clients. Confidentiality and duty of care in managing all aspects of the transactions related to such relationships and contracts are a significant element in the services and goods provided. Therefore any regulation which is likely to result in a breach of confidentiality is seen as a significant threat to the customer/client/third party relationship and the ability to fulfil contracts. Overseas competitors will have a competitive advantage when they are not subject to such regulation or protocols.

Release of information, (plain text or ciphered text plus encryption keys or access passwords) to anyone outside of the commercial organisation will immediately erode the trust relationship between the commercial organisation and intermediaries, agents, third parties, clients and customers. This will result in those clients and customers for whom confidentiality is paramount moving their transactions off shore. A good example is the growth of on-line auctions where customers specifically want anonymity in their transactions.

Applicability of RIP

Exploitation of e-commerce means that commercial organisations are increasingly administering processes on behalf of third parties and providing services to intermediaries, agents, third parties, clients and customers as a value added service beyond the commercial offering. For example in the administration and provision of insurance an insurer may provide an independent financial adviser (IFA) access to the insurers systems which will permit the IFA to send communications to the customer or other parties either as part of that contract or as a value added capability. This value-added service is not part of the contract or subject to charges but is provided as a means of retaining the relationship. If such "free" value added services result in the commercial organisation being included, say, within the definition of being an ISP they would therefore be subject to the provisions of the act.

The definition of communications data, and the ease with which the scope of such data can be changed without explicit consultation means there is uncertainty in the scope and applicability of the intention of the act

Warrants & Tipping Off

Assuming commercial organisations have the technical infrastructure in place to respond to warrants there are significant issues for those organisations who have no had experience of interception of communications. These are

- Training of staff to accept and handle requests has no commercial benefit and a direct cost.
- Ensuring there are caveats in contracts or notices to intermediaries, agents, third parties, clients and customers of the situations in which disclosures are liable to occur.
- The lack of any ability to challenge warrants and the risk of being duped into accepting a warrant. Where junior staff have been served with the warrant and cannot check with other staff because of the tipping off rules they are likely to accede to the request without challenge. To authenticate a request will be difficult for inexperienced staff.

RIP's role in forcing UK operations to move off-shore

The issues arising from RIP relating to trust and confidence in the commercial environment have already had the effect of prompting a shift from UK based operations to off-shore operations, with a consequent loss to the UK economy. Indeed, some countries have capitalised on RIP by actively promoting their own, more liberal, jurisdictions. Brendan Tuohy, senior spokesman for the Irish Department of Public Enterprise says the protection of all encryption keys was "a fundamental principle of the e-commerce Bill and an e-commerce environment and an important part of our e-commerce philosophy." (Irish Times 25th March 2000)

The Global Internet Project Encryption Summit on April 7th 1997 in London was addressed by the Heads of Global Security for (among others) IBM and General Motors (as well as DTI on UK policy). General Motors {such as the UK and US banks and law firms operating in the Far East) had no problem securing permission to use strong encryption in (for example) China, provided the US Government could not read it either. This scenario applies equally to the UK.

Over the past few months, UK-based operations have been pressured to set up confidentiality operations outside the UK for their overseas clients/customers/partners because of the expectation that overseas governments will demand the kinds of access that the RIP Bill might appear to give to UK agencies. These are being created in locations where the Government does not intend to claim such powers and/or makes their exercise illegal (so as to formally block attempts by other governments to claim access).

Government reassurances notwithstanding, the legal advice being provided to the City and its clients is based strictly on the text of the Bill. The definition of who is covered is "inclusive" rather than exclusive. It does not say who is NOT covered. Therefore lawyers are inclined to advise their clients that they are liable to be covered and should not take risks.

The advice being provided to companies is that the way for a "reputable" organisation to handle its legal responsibilities (including those to overseas clients) is either to always hold copies of any internationally used confidentiality keys (and state that these will be available to UK legal authorities under the Bill) or to never hold these (e.g. to use technology which does not store them after transmission in which they are used or, if it does, to ensure that they are split over one or more off-shore locations to which there is no access other than due legal process in all the relevant jurisdictions).

Since it is now prohibitively expensive (and all but impractical) to be certain of holding the relevant keys, the practical advice is commonly that the latter route is the best way of avoiding potential risk/liability. In

other words the confidentiality keys will no longer be accessible from the UK. This has, of course, consequences for the operations which use those keys.

The Home Office has consistently denied that these factors have emerged in the commercial environment, but Ministers appear to have failed to grasp the reality that companies traditionally see no advantage in going public. Instead, companies tend to conduct their operations quietly, acting in the best interests of their shareholders and clients, including those overseas.

Many companies believe the best way forward seems to be for the House Of Lords to act as a true revising chamber and identify the amendments necessary to identify who is NOT covered so that those doing business through legitimate operations based in the UK can have faith that their confidentiality will not be compromised - other than by the provision of plain text by court order.

Further Legal Instability : Rip And The European Convention On Human Rights

On the balance of legal opinion, RIP is incompatible with the European Convention on Human Rights. Under the Human Rights Act 1998, legislation must meet several convention requirements such as respect for private life and the right to a fair trial. While the Government has claimed RIP passes this test, it refuses to release any legal advice substantiating this claim. Barrister Time Eicke and former Law Commissioner Professor Jack Beatson QC have concluded in a legal opinion that it does not.

There are several areas of difficulty. Part III places the burden of proving that a key subject to a RIP warrant is no longer available upon the defendant. But proving that someone has forgotten a password is logically impossible. It also places those users following the good security practice of regularly changing keys and passwords, as required by the Data Protection Act 1998, in the invidious position of being more likely to lose access to that information. The right to a fair trail is further undermined by the lack of independent judicial oversight in issuing warrants.

The ECHR only allows interference with an individual's correspondence under strict tests of proportionality. Part III allows a warrant to be issued for any key "likely to be of value for purposes connected with the exercise or performance by any public authority of any statutory power or statutory duty." This is simply inadequate for allowing such severe interference in ECHR rights. Nor is any time limit on a warrant, or adequate oversight, required by the Bill.

The overall effect of these conflicts is to create uncertainty over the interpretation of RIP by the courts. Under the Human Rights Act, they may declare provisions of a Bill to be incompatible with the ECHR, or read them in a way that is compatible with Convention rights. The result is an unpredictable legal framework that will only be clarified after lengthy and expensive litigation that is likely to be appealed through the Court of Appeal, the House of Lords and possibly to the European Court of Human Rights.

Interception Costs

Commercial organisations who provide goods or services other than public ISP services but who are "caught" within the Act's definition of an ISP's will be expected to make arrangements for interception. The costs of making such arrangements can be significant even if no actual equipment has to be installed to achieve interception. The administrative costs of such investigations are often several hundred pounds per hour and if done in an ad hoc manner often involve significant effort. For example when administering subject access under the 1998 Data Protection Act it is common to incur costs of the order of five thousand pounds when using ad hoc processes. To establish regular processes requires investment in hardware and the development of software together with supporting administrative procedures. If these have no direct commercial purpose then the costs will have to be absorbed within the operation. With the multiplicity of relationships, processes and application, each of which will require similar arrangements, will add significantly to operating costs.

For those considering investment in e-commerce or extending their exploitation of e-commerce, there will be unknown technical implementation requirements and costs to be included, which may constrain both the possible technical solutions and the legal framework within which services are provided.

No provision for these development and investment costs are made within the RIP Bill other than for directly attributable collection costs.

The Core Problem : Home Office Incompatibility With Commerce

The basis of these business problems stems largely from an apparent inability within the Home Office to understand the commercial operating environment.

It is now well known within the business community that there exists a serious communications gap between the law enforcement agencies and the electronic security operations of the private sector. The main reason is the lack of career continuity and thus in-house expertise among those in the electronic investigation teams of the law enforcement agencies, reinforced by the low priority these have received over the ten years since the first was created.

The cost to industry of electronic security, including combating the regular stream of hacking and vandalism attacks, let alone industrial espionage and attempted fraud, appears almost unknown to the Home Office -mainly because it is almost never reported or collated. For example few appear to appreciate the scale of the damage down by the Love Bug to graphics and engineering design houses and the music industry (it corrupted many JPEG as well as MPEG files). It costs around £250,000 to run a 24by7by52 fire-wall with only one man on duty at any given time. Most have several. The Computer Crime Unit that is the UK end of the G8 Global Response Team has fewer Officers than would be needed to man the firewall of one major bank. Many Banks and Insurance companies also have on-call arrangements with the investigation and forensic teams of the main international accounting firms (e.g. KPMG) and "recovery" operations (e.g. Control Risks).

At the PITCOM meeting on E-Crime on 5th June 2000 it was pointed out (in the vote of thanks) that the e-fraud investigation team of one bank alone is several times larger than all the Computer Crime Units of all the UK police forces added together (and that was before including their electronic security team). Another important factor in the failure of RIP stems from the generally held view within the Home Office that the debate over the RIP Bill is different to that over Keys in Escrow, E-Crime or E-warfare. Industry and the City, on the other hand, see these as integrated issues.

Summary of key business implications

The specific areas of commercial and economic activity which are likely to be adversely affected by RIP are:

i. Direct costs of interception equipment and support

ii. Recurrent cost of equipment design to meet changing RIP requirements

iii. Costs associated with securing legal and professional advice

iv. Additional insurance costs

v. Displacement of investment in new operations to non UK jurisdictions

vi. Loss of existing UK based operations to off-shore locations

vii. Loss of confidence and trust amongst e-commerce consumers

viii. Loss of UK share in the global e-commerce market

ix. Losses arising from inability to create value added services

x. Opportunity costs arising from the inefficient use of specialist staff

xi. Civil litigation arising from breach of confidence or misuse of keys

xii. Cost of management and retention of revoked keys

xiii. Inhibition to the development of new products and services

xiv. Losses arising from technology lag between the UK and overseas

xv. Additional costs and licence fees for imported equipment where UK specific equipment versions are required

xvi. Loss of international contracts due to an inability of UK operators to guarantee equivalent levels of security

xvii. Liability arising from exposure in other jurisdictions to actions required in the UK to comply with the RIP Bill.

Assessment of economic cost

The impact of RIP on the UK business sector and the economy can be measured by the impact it will have on :

a) The functioning of individual businesses,

b) The nature of business-to-business relationships;

c) Direct costs associated with meeting the requirements of the legislation;

d) The overall level of consumer confidence in e-commerce;

e) Investor confidence

Only a few of the seventeen factors listed above which are likely to have a key bearing on the economic environment can be measured. Amongst the most significant of these are:

The direct cost to ISP's

The economic impact on ISPs has been assessed earlier in this report as being in the magnitude of £50 - £60 million per year, based on current traffic. However, this figure is based on a narrow interpretation of the Bill, and does not, in its baseline estimate, take into account the growth of the Internet, and the expanded use of part I to such media as mobile phones and interactive television. These additional forms of communication should increase the baseline cost by twenty per cent per year.

Internet traffic is currently increasing by around 600 - 1,200 per cent per year (traffic across the members of the London Internet Exchange (LINX) is doubling every 100 days). This will to some extent reflect proportionately in the cost of part I surveillance requirements. Taking into account the natural reduction in price of surveillance software and hardware products, and the expected slowing in the growth of ISPs, a five year projection for the population of organisations caught by the legislation would be :

2001	60m
2002	85m
2003	120m
2004	165m
2005	210m

Total actual cost over five years : £640 million

These figures do not take into account substantial opportunity costs arising from the inefficient use of specialist staff in an extremely tight IT labour market.

Costs arising from the imposition of technical design requirements

The government's stated intention to make Britain the most desirable place on earth for e-commerce does not carry with it a commitment to make the UK the most self-reliant environment in the world. Britain relies to a large extent on the import of large volumes of hardware and software to support the local market. Any equipment imported into the UK must be compatible with local laws and conditions. Invariably, the more a countries local environment is at variance with the global environment, the greater the range of associated costs and penalties. It is in this respect that RIP, and its consequent technical compliance requirements, will incur costs.

Information supplied by non-UK IT suppliers indicates that the provisions of RIP may incur additional costs that will result in a 5 - 10 per cent increase in the cost of licences for modified equipment and software (see section "design costs" above). As the Internet reaches maturity, and as it merges with various forms of media and telecommunications, the number of imported products subject to the provisions of RIP are likely to increase substantially.

Estimates of the overall cost to the UK vary considerably, but are likely to reach more than £1 billion a year by 2002.

Other direct costs to business

Most business contacted during the preparation of this report expressed concern about the following RIP related direct costs to their operations:

- Costs associated with securing legal and professional advice
- Additional insurance costs arising from RIP related liability
- Losses arising from inability to create value added services
- Opportunity costs arising from the inefficient use of specialist staff
- Civil litigation arising from breach of confidence or misuse of keys
- Cost of management and retention of revoked keys

Such factors are likely to be considered by a surprisingly large number of companies. One of the reasons for this concern is the scope of a "public telecommunications service" liable to be required to provide interception capabilities. More and more companies are introducing services to the public that exploit the internet, and replicate many of the services offered by ISPs and content service providers. There is general concern as to whether they are liable for a Notice to incorporate interception capabilities. Informal discussion suggests that only certain types of service (particularly those that enable persons to

communicate) are intended to be covered (as appears to be the intent of paragraph (b) under "postal service"). However, the definition of "telecommunication system" in Clause 2 includes provision of "communications", which is defined in Clause 72 as "signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation and control of any apparatus". This would seem to cover every form of service provision including web servers (thing to person), communication between processes and even remote activation of devices. While Clause 2 (3) excludes broadcast for general reception, this does not seem to exclude internet services such as web servers since they do not broadcast, but transfer information on the request of the caller. Words are needed to limit the scope of this definition if that is the intention of the government.

A number of SME's have informally estimated that these factors could cost each organisation anywhere between £100,000 and £500,000 annually. If these figures are realistic, it is likely that these costs, when calculated across the ICT and finance sectors, will amount to at least £1 billion pounds per annum by 2003.

Erosion of the UK share in the global e-commerce market

The UK government has accepted conventional projections that the global e-commerce market will, in 2003, reach £800 billion. In its promotion of Britain as the most desirable place in the world to conduct e-commerce, the DTI says the UK is uniquely placed, in terms of language, culture and the legal environment, to reap a significant share of this market.

The precise target for this share is unclear, though around 5 per cent is generally regarded as sustainable, in spite of increased competition from other European countries. This share would equate to around £40 billion by 2003, levelling to £55 billion by 2005.

An international benchmarking study published in 1999 concluded that European countries, in particular, have seen strong growth in terms of ownership of ICT hardware and applications, closing the gap with the US and Japan. Moreover the UK's position as the leader amongst the benchmarked European countries is now being challenged. While the UK is still ahead of France and Italy, very rapid growth in Germany (perhaps driven by recent telecommunications regulation) has put it on a par with the UK on most measures of ICT uptake. The development of e-commerce parallels these trends.

Achieving a substantial share under global market conditions will depend to a large extent on attracting foreign investment for new e-commerce ventures. It will also depend on maintaining local processing operations within the UK. The evidence presented to this report indicates that neither circumstance will prevail. The spectre of the RIP provisions have already caused VC companies, multi-nationals and investors outside the UK to favour other jurisdictions. Local companies, including banks, have already made clear their intention to move some operations off-shore.

On the basis of current opinion, between 20 and 30 per cent of investment in e-commerce and processing operations will be lost to overseas jurisdictions. In consequence, 20 – 30 per cent of e-commerce trade will be lost to overseas jurisdictions. Based on the lower estimate, the UK is likely to lose the following value in e-commerce transactions :

2001	£2 bn
2002	£4 bn
2003	£8 bn
2004	£10 bn
2005	£11 bn

The five year total of e-commerce leakage to overseas jurisdictions is therefore in the order of £35 billion.

Section C: Further Analysis and Implications

Section C.1 INTERNATIONAL DIMENSIONS

At the recent Paris summit for the G8 on cybercrime, two imperatives were discussed in dealing with investigative methods: co-operation between government and industry, and international synergy. This report has thus far investigated the *co-operation* with industry in the sense of dictating to industry the form and nature of their operations by the RIP bill. What remains is how the RIP bill fits into the international dimension.

This section on International Dimensions will first continue discussion on the reverse-burden of force key-disclosure and discuss the lack of international consensus on its viability. Meanwhile for interception of Internet communications and communications data, the case of Russia will be presented as it is the only other democratic country with such an invasive and costly scheme. This scheme will be discused in detail as well as the associated costs, and investment concerns.

C.1.1 International Survey on Lawful Access And Forced Disclosure Of Encryption

Following the rejection of key escrow, the new approach being considered by many governments is to demand "lawful access" to encryption keys. Under this approach individuals would be required to disclose keys to law enforcement agencies or face criminal penalties for failure to assist in a law enforcement investigation. So far, only a few countries have implemented such provisions.

The March 1997 OECD *Cryptography Policy: The Guidelines And The Issues* report outlined agreed guidelines for member states encryption policy. These guidelines noted but did not endorse the lawful access principle. The Guidelines principle states:

> National cryptography policies *may* allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible. [ed. emphasis added]

This was a very contentious issue in the OECD. The OECD considered and rejected support for the lawful access to encryption keys. As a result, this is the only principle within the entire report that did not state that members states *"shall"* adopt as a policy, and indicated rather that member states *may* allow for lawful access.

At the Denver Summit in June 1997, the G-8 supported access, however. It recommended that every country adopt "Lawful government access to prevent and investigate acts of terrorism and to find a mechanism to cooperate internationally in implementing such policies." The Draft Council of Europe Cyber-crime treaty also proposes lawful access.

Only Singapore and Malaysia have enacted laws that would require users to disclose their keys or face criminal penalties. In both of those countries, police have the power to fine and imprison users who do not provide the keys or the plaintext of files or communications to police. A similar bill is pending in India. It is within this group of countries that the UK is about to enter.

In the United States, Belgium and the Netherlands, bills are pending that would require third parties to release encryption keys if held (under the older Trusted Third Party scheme) but would not require a person to incriminate himself.

A number of countries including Ireland, Sweden, Finland, and Denmark suggested that the government would consider lawful access provisions following the release of the OECD Guidelines. Thus far, none have adopted it. In Ireland a draft Electronic Commerce Bill has recently been published which would force individuals to provide access to plaintext but recommends against forced disclosure of keys. In Canada, an interministerial committee headed by Justice Canada is examining possible legislation. Other countries such as Denmark have decided against adopting such policies.

The Right Against Self-incrimination

Such approaches raise issues involving the right against self-incrimination, which is respected in many countries worldwide. The privilege against self incrimination forbids a government official from compelling a person to testify against himself. It has a long history in law originally developing from Roman and Canon law and was subsequently adopted by the Common law.[5]

In the United States, this issue has not been directly addressed by any courts yet but many legal scholars believe that it would not be permissible under the 5th Amendment to the Constitution to force an individual to disclose an encryption key or passcode that was not written down anywhere.[6]

Many European legal scholars also believe that requiring disclosure violates the European Convention on Human Rights (ECHR), as FIPR and Justice have indicated with their commissioned legal audits, as discussed above. Such a decision relating to the ECHR will apply to all member states; if the UK decides to continue with this reverse-burden idea, it may well go at it alone within the EU. The European Court of Human Rights has stated that the right of any "person charged" to remain silent and the right not to incriminate himself are generally recognized international standards which lie at the heart of the notion of a fair procedure under Article 6 of the European Convention on Human Rights. The burden of proof cannot be reversed for the suspect to provide the requested evidence or prove his/her innocence.[7] Article 8 of Convention, which protects the right to respect for private life and correspondence also sets out limits on surveillance that would affect interception.

In other countries, this concern is also raised. The New Zealand Law Commission noted recently that on the issue of lawful access, it will be difficult to compel people to disclose encryption keys:

> We note that the difficulty in compelling a person to disclose the means of decryption, or the plain text of the document itself, will need to be given considerable thought; as will the question of an appropriate sanction in the event that disclosure is not made. In that regard, the disclosure of something held in one's head is somewhat different in kind to the provision of DNA samples. Ultimately, any view formed on this issue will need to recognise that a private key may be held in the memory of a human being, rather than located in an electronic or paper based record.[8]

In Australia the Walsh Report, written by the former director of the Australian intelligence agency, also recommended against the "lawful access" requirement stating:

> 1.2.27 Invocation of the principle of non self-incrimination is likely to prove an obstacle to efforts by law enforcement agencies to obtain encryption keys by search warrants or orders made by courts and tribunals.[9]

This is because some governments are forced to follow constitutions and other democratic legal regimes.

C.1.2 SORM: From Russia With Lessons

In April 2000 a subcollection of the authors of this report presented at a conference in Moscow to discuss privacy and technology with Russian human rights groups. What was supposed to be an education for the Russian NGOs turned out to have a second, unforeseen, type of education: we learned how

---

[5] See R. H. Helmholz, "Self-Incrimination: The Role of the European Ius Commune", 65 NYU L Rev 962 (1990). See also L. Levy, Origins of the Fifth Amendment: The Right Against Self-Incrimination (2d ed. 1986).

[6] Doe v United States, 487 US 201, 219 (1988), Justice Stevens wrote in dissent, "[a defendant] may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe--by word or deed." See Kathleen M. Sullivan, "Privacy in the Digital Age: Encryption and Mandatory Access" before the Subcommittee on the Constitution Federalism and Property Rights, Committee on the Judiciary, United States Senate, March 17, 1998; Greg S. Sergienko, *Self Incrimination and Cryptographic Keys*, 2 RICH. J.L. & TECH. 1 (1996) <http://www.richmond.edu/jolt/v2i1/sergienko.html>, For the US government view, see Phillip R. Reitinger, Compelled Production of Plaintext and Keys, The University of Chicago, 1996 U Chi Legal F 171

[7] See the following judgments of the Court: Funke v. France, 25 February 1993, Series A no. 256-A, p. 22, ß 44; John Murray v. the United Kingdom, 8 February 1996, Reports of Judgments and Decisions 1996-I, p. 49, ß 45; and Saunders v. the United Kingdom, 17 December 1996, Reports 1996-VI, p. 2064, ß 68; Serves v. France, 20 October, 1997, Reports 1997-VI). Our thanks to Yaman Akdeniz for this information.

[8] New Zealand Law Commission, "Electronic Commerce Part Two: A basic legal framework", November 1999.

[9] AG Letter Review of Policy relating to Encryption Technologies (Walsh Report), October 10, 1996. <http://www.efa.org.au/Issues/Crypto/Walsh/index.htm>

Russia was actually leading the world with its efforts in surveillance on the Internet, particularly through of interception of communications on the Internet. The parallels become even more insidious as the UK moves forward with RIP, and the Council of Europe with its Draft Convention on Cybercrime, and the G8 with its initiatives in cybercrime, of which Russian is a member, if not an educator.

Among various initiatives, the most relevant to Section I of the RIP bill is Russia's SORM*: Sistema Operativno-Rozysknykh Meropriyatii*, or "System of Ensuring Investigative Activity". Introduced in its original form in 1994, SORM-1 gave the FSB, the re-born KGB, the right to monitor all telecommunications transmissions, provided the security service first obtained a *court order*. Under SORM-2, in July 1998 the additional regulation outlined how internet service providers were legally bound to install, at their expense, a black box that linked the ISP activity with the FSB.[10]

Similar motivations, and speech patterns, arose in support of this measure. As a department head of the Communications Ministry stated:

> "Speaking about the incorporation of SORM into the Russian communications network, we are speaking not about establishing a system of global surveillance of the Internet, or total control of the information that is transmitted via the global network. Instead, we are speaking about [monitoring] individual cases according to the law.
>
> Security organs and special forces have the right — and now the capability — to monitor private correspondence and telephone conversations of individual citizens in the name of establishing legal order."[11]

"Legal Order", as the communications ministry official states, need not be merely in the name of public safety. As the Liberal-Democrat front-bench spokesperson on RIP Bill, Richard Allen, warned of at a March 2000 London conference on RIP, powers expand once powers are granted and government ideas changed: he warned of the next time party power shifted in the UK and the Tories would extend monitoring for preventing benefit-fraud, for example. This was exactly the case in Russia. An obscure legislation approved by President Vladimir Putin extended the government agencies that have access to communications and traffic intercepts from what was originally only the FSB to include *six* other organisations, including the Border Guards, and the tax police. As Yelena Bonner, human rights advocate and wife of the late Soviet dissident Andrei Sakharov, remarked on this development:

> "This means Russia has officially become a police state. And this war-time police state came about unnoticed when Putin rose to power on Dec. 31."[12]

Powers are rarely restricted once developed; rather they are often stretched.

As Western countries discuss developing a *dialogue* with industry in the name of preventing cybercrime (particularly under the G8), such *co-operation* is quite opaque in Russia. While the media has tried to penetrate this issue and discuss SORM-2 with ISP officials, generally the ISPs are unwilling to be engaged on this issue[13] while many of them have already quietly complied.[14] SORM-2 in 1999 still had "not yet passed the legal examination of the Ministry of Justice, in fact, [but] the FSB had already introduced the

---

[10] There is some uncertainty as to when the regulations were actually introduced. In an email from Sergei Smirnov of the Human Rights Online, a Russian NGO, he says of SORM-1's supposed '1995' release: "They say, 1994. Since it has not been widely introduced to public we used to call it "first known in 1994"." As for SORM-2, he continues: "The first evidences of SORM-2 appeared on the Net in the beginning of summer 1998. However, the paper itself might appear earlier, we don't know exactly when." There is a limited form of openness in Russian government procedures, it seems. Much of this section was possible due to the assistance of Sergei Smirnov, and the work he has done over the past few years in Russia in making this knowledge available.

[11] Alexei Rokotyan, head of the electronic communications department, Moscow Times, Government Admits to Internet Watching Using SORM, Jen Tracy, February 18, 2000.

[12] Moscow Times, Police Get Window Of Access To E-mail, By Jen Tracy, February 21, 2000.

[13] CNN.com, Russian Web site fights government monitoring effort, August 11, 1998, Web posted at: 12:31 p.m. EDT (1631 GMT), by Mike Hanna.

[14] Moscow Times, Police Get Window Of Access To E-mail, By Jen Tracy, February 21, 2000.

initiative practically everywhere", according to Nail Murzakhanov, the general director of a Russian ISP, Bayard-Slavia Communications.[15]

The details to the Russian SORM bear a striking similarity to the UK's RIP. According to S1.3 of the 1998 *Technical Requirements To The System Of Technical Means Providing For The Fulfillment Of Efficient Research Measures In The Documented Telecommunications Networks, Approved by Deputy Director Federal Security Service A.A. Bespalov*:

> SORM should provide for reading of all information (both incoming and outgoing) belonging to the specific subscribers of the network(s) in question.

The requirements are that all network providers must have black boxes in their operation centres that provide a secure link to share communications data with the Data Collection Centre, i.e. the FSB. The data that is collected includes the suscribers database (registration date of the client, addresses), statistical information, traffic contents belonging to specific suscribers, subscriber telephone details (CLID), real-time information transmitted via the network carrier and belonging to specific subscribers. An additional requirement is that the SORM reaction time from a command transmission for information from the DCC "should not exceed 30 seconds" (3.8).

The similarity with the UK is already striking, as the Home Office argues that the technical details will be later sorted out: SORM-2's authors need not seek approval from Parliament because Russia's *Law on Investigative Activity* (RIP?) already grants them the power to observe private correspondence. The Russian *authorities* see SORM-2 merely as an implementation of *their* rights, as granted in the Russian version of RIP, and therefore do not need the *support* of Parliament.

The technical implementation of RIP is bound to be similar to SORM-2. When we in the UK finally observe, and dare to question the technical details to RIP we will be shocked to see that RIP will already be law, and thus negotiations will already be over. This has been the Home Office's line of reasoning whenever we raise technical concerns, as the Home Office responds that we will deal with these issues of implementation in Working Groups *upon the passing of the RIP bill*, and this is inscribed in RIP Section 62. The UK Government strategy is a modelling of Russia's, with alarming perfection.

SORM: Costs and Market Effects

The costs of SORM lie with the provider. The provider was responsible for paying the costs of installing the equipment (an initial cost estimate of $25,000, and could ultimately have cost $120,000) and wiring up the local FSB office with a high-speed leased line (required to be at no less than the maximum speed possible with current technology, with an estimated cost of about $1,000 per month for the line to the FSB). The high assocated costs were a strain on smaller ISPs; thus, the rumors were that SORM, besides being initiated by the FSB, was being co-sponsored by big ISPs. As a Russian Internet expert, Anatoly Levenchuk, said:

> "Most Internet providers in Moscow, including all of the large providers and many in the provinces, have opened a hole for security agents to peep at traffic."[16]

Failing to implement SORM, is even more dangerous, from a business perspective. According to a consultant for the State Duma Security Council, and a supporter of SORM-2, Yelena Volchinskaya states:

> "All providers are gradually starting to implement SORM, because their licenses will be revoked if they don't."[17]

This has indeed occurred in one public case.

---

[15] The Wall Street Journal Interactive Edition, Russian ISP Finds Court Victory Sometimes Is No Victory at All, By Jeanette Borzo, October 5, 1999.

[16] Alexander Moskalyuk, Government Control of Information Technologies: the Post-Soviet Experience, paper submitted to the Civic Education Project, Date: Wed, 12 Apr 2000 19:04:02 -0700 to Declan McCullagh.

[17] Moscow Times, FSB Now Wired to Read Your E-Mail, By Jen Tracy, December 7, 1999.

An ISP in southern Volgograd, Bayard-Slavia Communications refused to implement SORM; this resulted in its main communication line being cut off through concealed actions by the FSB, and faced threats of fines from government officials (including the tax police), and lost their telecommunications provider license. The ISP took the case to court in order to get their license back. The telecommunications body rescinded the suspension as a result of the court case. As the Wall Street Journal sollicited comments from the industry regarding SORM-2 and the Bayard-Slavia case:

> "It has real ramifications for investor interests in this part of the world," says David Bain, chief executive officer of Global Information Services & Technologies Inc., an Arlington, Va., consulting and publishing company.
>
> "Seventy years of totalitarianism are not so easy to overcome, even if we assume that the state methods have changed," says Michael Novikov, the chief executive officer and founder of Admin Ltd., an Internet and e-commerce consulting firm in St. Petersburg.

According to the general director of Bayard-Slavia, it is the press coverage that keeps his company alive:

"The interest of the public, attracted by the press, has prevented the FSB and Gosvyaznadzor from killing my company."[18]

SORM: International lessons taught, lessons learned

SORM has never been passed in the Russian Parliament. In the Ukraine, when the president and the security agencies tried to implement SORM by decree, it was suprisingly vetoed by the parliament. Meanwhile, in a recent speech, George Soros spoke wishfully regarding investments into the Russian Internet industry, with reluctance directly focussed on the FSB:

> "Russia is lagging behind the world, and therefore I think the opportunity in Russia is very great, unless the considerations of national security interferes with that development."[19]

Soros may wish to look in to the Ukraine for investment, instead of Russia and the UK.

Ironically, SORM is not without its opposition, nor challenges, however. A letter filed in September to the Minister of Justice stated that legally, SORM contradicts with the Russian Constitution, particularly Article 23 which guarantees the right to the secrecy of communication.[20] The irony is that the UK government is rushing to get the RIP measures passed before the UK enacts the European Convention of Human Rights, amongst other reasons, to pre-empt such legal *contradictions.*

The UK may be learning from the Russian experience. Where did Russia learn its methods? Barry Steinhardt, the Deputy Director of the American Civil Liberties Union (ACLU), recounts:

> "I had a conversation with a couple of members of the Duma who said they had meetings with people from the U.S. Justice Department in Russia who were there teaching them how to do this."[21]

Other such meetings have occurred. The G8, for example have been moving towards creating cybercrime agreements among member countries (and others, as was revealed at the May 2000 Summit hosted happily by the French, who now hold the presidency of the EU). This G8 initiative actually began in Moscow in October 1999 in an attempt to reach an agreement on practical measures to combat crime.[22] There, the G8 countries agreed to begin drafting national legislation that will require ISPs and telecom companies to maintain, preserve, and hand over log files to law enforcement agencies; is it merely an

---

[18] The Wall Street Journal Interactive Edition, Russian ISP Finds Court Victory Sometimes Is No Victory at All, By Jeanette Borzo, October 5, 1999.

[19] Reuters, Soros Still Bullish on Russia, 8:15 a.m. Jun. 8, 2000 PDT on Wired.com.

[20] Citizens' Watch, Filed Letter to Yuri Chaika, Minister of Justice of the Russian Federation, September 1999, No. 54/1-99.

[21] Milwaukee Journal Sentinel, June 6, 2000 Tuesday, Cyberfear leading to international invasion of privacy, Robyn Blumner of the St. Petersburg Times.

[22] G-8 Talks Traceback in Moscow, by Holly Porteous, CanCERT™ Bulletin (Vol.2, No.5, Dec. 1999).

irony that such an agreement occurred within the only G8 country at the time to have such measures under SORM? Four months later the UK follows up on that promise and releases RIP, or SORM-UK.

The Wall Street Journal in 1999 reported on Russia's SORM system with concern, and pity. The WSJ concluded:

> "Next time you think a Net community is getting a raw deal, spare a thought for the Russians."[23]

The UK seems slated to be the next country to receive such pity, but not sent from the governments of Canada, France, Germany, Italy, Japan, and the US as they watch with interest, and learn.

International Conclusions

The UK is following the path set by Russia when it comes to interception almost exactly, and may suffer some of the fate of Russia as investors become concerned about heightened surveillance within the infrastructure. Ironically, Russia has a constitution, and thus SORM may be revoked by a legal decision; the UK Government has ignored all such possibilities.

As for the forced disclosure of encryption keys, apart from aiming to become members of an elite group of countries such as Malaysia and Singapore, the UK is treading into unknown and uncertain waters. That is, already pursuing an acknowledged loophole within the agreed OECD Cryptography Policy guidelines, the UK is facing a direct confrontation with the ECHR. According to legal analysis, however, such an effort is doomed to fail, at the cost of time and effort within the UK. The UK seems prepared to follow the G8 recommendations while ignoring its own domestic laws and rights despite reports from other countries that forced disclosure is impractical, if not impossible within a democratic legal regime.

Since there are countries that are not willing to pursue forced disclosure, or countries that are more willing to adhere to the established rights and laws, it is not within the interests of companies to establish their services within the UK. While some governments, such as the US and France may discuss forced-disclosure and access to traffic data within the forum of the G8, every initiative will encounter opposition from within their countries, not only from civil liberties campaigners and industry advocates, but also from their own legal regimes that protect individual rights. Meanwhile as other countries work towards costly infrastructures of surveillance, modelling Russia's SORM and the UK Government's RIP bill, in addition to forced-disclosure of encryption keys, the UK is actually forging new ground and drawing the map for these regimes who are willing to forego fundamental human rights, and as an international financier puts it, allow the considerations of national security to interfere with the development of the Internet, and thus discouraging investment.

Those living within free countries may be sparing a thought for Russia and the UK; but the citizens of less democratic regimes will hardly be sparing a free thought towards us as their own regimes follow the UK's example with the aim to oppress. Only when all countries live under this *oppression* may investors return to the UK.

[23] The Wall Street Journal Europe, Ideas And Trends --- Russia: E-Spooks, Tue, 20 Apr 1999.

Section C.2 TECHNICAL INFEASIBILITY

The powers provided by RIP may be almost entirely ineffective, given current developments in security technologies. This section describes likely problems in law-enforcement access to communications and stored data, and procedural measures companies would be advised to take to further reduce the impact of RIP.

Communications

Many businesses already have "always-on" connections to the Internet. British Telecom's current rollout of ADSL, a low-cost high-bandwidth permanent Internet link, will encourage more to do so. This will encourage the use of online security techniques that are far less amenable to the interception powers of RIP.

Most current e-mail encryption software uses long-term keys. Once requisitioned under a decryption warrant, such keys often allow years' worth of messages to be decrypted. But online e-mail software can negotiate a new key for each message with its recipient, which is destroyed after its transmission. The next version of the most widely used Internet mail server, sendmail 8.12, contains this feature. Any such messages intercepted under warrant are unreadable ciphertext whose key cannot be recovered from anyone, as it no longer exists. Simply by default, the vast majority of messages sent to or from a British mail server will become so protected as this software is installed over the next year. Mail client software is already including these features, and will allow users to send messages directly to their recipients so that local mail servers are avoided.

These capabilities are already built into the most popular World Wide Web browsers and servers. While secure links are currently widespread for e-commerce transactions, they can be easily used for normal browsing. Web sites containing material that may be compromising to its readers are likely to quickly enable security facilities. "Anonymising" Web servers already provide a secure gateway through which subscribers can browse unseen by Web servers or interception facilities.

The greatest impact is likely to come from the deployment of security extensions to the Internet Protocol. These have been finalised by the Internet Engineering Task Force in the last 18 months, and are being built into Windows, Linux and other popular operating systems. They will secure all Internet traffic in the manner described above.

Further enhancements allow even the existence of a communication to be hidden. Systems such as the US Naval Research Laboratory's Onion Routing, and Zero Knowledge System's Freedom, route encrypted Internet packets through a number of different servers to disguise their origin and destination. Only by compromising every server in the link, likely on several different continents, can this information be discovered.

Stored data

Encrypted disk software is already widespread. Decryption warrants can demand the password to a disk from its owner. But a new generation of "steganographic filesystems" allows different files to be encrypted on a disk using different passwords. The existence of these different files and passwords is invisible to the most detailed forensic examination of a machine. There is therefore nothing to prevent a user revealing one password that protects relatively unimportant files, whilst concealing the existence of other information. Such a filesystem is already available for Linux; RIP can only encourage its implementation for Windows.

The Internet also provides a route to secure overseas storage. Files can be stored overseas beyond the reach of RIP warrants. Their existence can be hidden using secure communications links.

Finally, smartcards and other similar hardware devices allow cryptographic keys to be stored in a way that even their user cannot extract them. The device will decrypt data presented to it, but will resist all efforts to access its keys. While current devices are less than 100% effective in this regard, techniques to improve

their security are a very active area of research and development. A user may be unable to comply with demands for keys stored on these devices.

Procedural difficulties

Companies should take a number of organisational steps to minimise the impact of RIP on corporate security.

Multinational businesses can minimise their exposure to particular jurisdictions by splitting information between them. A rarely used, high value key -- such as a company's root certification key -- could require the approval of a number of corporate officers in different countries for access. Each should be required to verify that the others are not operating under legal compulsion before giving assent.

Company security functions should also be judiciously sited. Any sensitive key material should be kept out of the reach of key warrants in a country like Denmark that has rejected them.

Keys that are seized under warrant must be immediately revoked to prevent their use to protect any further information. While the recipient of a warrant may be required to keep its existence secret, the Home Office has confirmed that such keys may be revoked. Companies must have procedures in place to allow immediate revocation and notification throughout the organisation. They must ensure that designated corporate officers are able to revoke keys when an employee has been unable to do so. Ideally, their software should enforce the revocation of a key before its disclosure.

The high cost of countermeasures

Given its ineffectiveness, RIP will inevitably only be the first step in a prolonged "arms race" between law enforcement agencies and their surveillance targets. Just as RIP has been justified as merely an update of existing interception legislation, increasingly restrictive measures are likely to be proposed simply to maintain the effectiveness of the RIP interception regime.

To have any impact, such measures would need to be restrictive indeed. Restrictions on security software functionality and the operation of the UK Internet, with random monitoring for enforcement, would be essential were RIP to have continued utility for law enforcement and intelligence agencies. Cheap secure communications can only encourage companies to avoid the cost and vulnerabilities introduced by such restrictions by moving increasing areas of corporate function away from Britain.

Meanwhile, the UK taxpayer, ISPs and UK company shareholders will be required to fund more and more baroque and expensive interception capabilities.

IMPLICATIONS AND CONCLUSIONS

The Home Office seems to have virtually ignored the economic impact of the RIP Bill. Whilst business is fully supportive of the need for efficient and effective policing of criminal activities, the Bill seems an extremely expensive yet ineffective method of doing so. It is likely to lead to loss of confidence in e-commerce, unacceptable costs to business and to the UK economy, confusion and uncertainty at numerous levels of business activity, and an onerous imposition on the rights of individuals.

These problems stem from a lack of understanding of the commercial operating environment by the Home Office. There is a serious communications gap between the law enforcement agencies and the electronic security operations of the private sector. The cost to industry of electronic security, including combating the regular stream of hacking and vandalism attacks, let alone industrial espionage and attempted fraud, appears almost unknown to the Home Office – mainly because it is almost never reported. The Computer Crime Unit that is the UK end of the G8 Global Response Team has fewer officers than would be needed to man the firewall of one major bank. The e-fraud investigation team of one bank is several times larger than the combined Computer Crime Units of all the UK police forces.

The definitions used in the Bill are excessively broad, leading to substantial doubt as to the level of exposure to cost, risk and disruption for business. Of even greater concern are the implications that arise as various agencies explore how this new framework might be 'stretched' in the future. The part III issue of the reverse burden of proof regarding lost or missing keys have important repercussions for business for the management and retention of revoked keys. These imponderables cast uncertainty over future investment decisions.

The Bill therefore imperils the government's intention of making Britain the most desirable place to trade electronically. As it stands, RIP is likely to create a legal environment which will inhibit investment, impede the evolution of e-commerce, impose direct and indirect costs on business and the consumer, diminish overall trust in e-commerce, disrupt business-to-business relationships, place UK companies at a competitive disadvantage, and create a range of uncertainties that will place a growing number of businesses in a precarious position. There is compelling evidence that the Bill will create a trend amongst UK firms to establish a range of operations offshore, whilst inhibiting the creation of, and investment in, new business functions in the UK.

The Bill would create an unpredictable legal framework. Protracted litigation will be required to determine whether part III contravenes the European Convention on Human Rights. Elements of part I may breach the Data Protection Act, while the execution of the Bill's provisions in both Parts I and III are likely to compromise a range of conditions relating to duty of care. Practical implications will depend to a great extent on the provisions in secondary legislation, and the scope of the Code of Practice. The fact that the government has failed to provide details of either has placed UK business at a great disadvantage in assessing the legislation.

The Bill also poses a number of unresolved questions in regard to both employment and company law. The Government may be deemed to be acting as a 'shadow director'. There are obvious questions about the potential civil liability of the company if the surrendered keys were used in such a way that an innocent third party suffered loss. The Bill is unclear about which officials, at what level, in which departments may seek access to encryption key material. Of greater importance is the lack of clarity in the Bill on the question of warrant procedure and validation.

There is considerable concern in the business community on the degree of individual and corporate liability flowing from exposure in other jurisdictions to actions potentially required in the UK to comply with the RIP Bill. If decryption keys are demanded using a Section 46 notice with an associated 'tipping-off' order, individuals working for multinational companies could be placed in a perilous position. They may have compromised the international transactional security of that organisation yet be directly barred from informing senior management of that exposure. Such an individual may be protected under UK law

for these actions but their exposure in other jurisdictions – particularly that of the parent company - is uncertain.

The compliance costs to ISPs alone were substantially underestimated by the Smith report, and a five year estimate will likely be in the order of £640 million. The overall financial implication of RIP, in terms both of losses and leakage from the UK economy, and of cost of implementation, may be in the order of £46 billion in the first five years of operation.