

The Regulation of Investigatory Powers Bill – The Provisions for Government Access to Keys

by Dr B. R Gladman for the Foundation of Information Policy Research (FIPR)

Abstract: The UK Government has put a Bill before Parliament which includes provisions giving a number of government and public authorities the power to demand copies of the encryption keys which UK citizens and companies use to protect their sensitive information. Because of the nature of modern cryptography many of the keys sought will belong to owners who are not themselves under any suspicion. This paper considers the consequences for such owners if their keys are revealed or stolen while in the custody of these authorities and concludes that many will face severe risks to their safety and security unless the authorities involved provide the strongest possible protection for all keys that are seized. Experience shows that the costs of such measures will be very high but the Government has given no indication of their scale and no evidence to show that the benefits of these proposals are sufficient to justify the very large costs which will be involved. The paper concludes that these aspects of the Bill are ill thought out and will either impose a large and possibly unjustified cost burden on UK taxpayers or create very significant risks to the safety and security of many of those whose keys are seized.

Introduction

1. On 10th February 2000, the UK government put a Bill before Parliament which, if enacted, will give a number of UK government and public authorities the right to obtain the encryption keys that UK citizens use to protect their information. The aim of this paper is to analyse a number of the consequences of implementing these provisions in order to determine whether these proposals are a sensible and realistic response to the potential difficulties that they are designed to counter.
2. The provisions for access to keys in the Regulation of Investigatory Powers (RIP) Bill will be referred to here as Government Access to Keys (GAK). The authorities who are to be given this access will be referred to collectively as 'GAK Authorities' (GAKA).

Public Key Cryptography

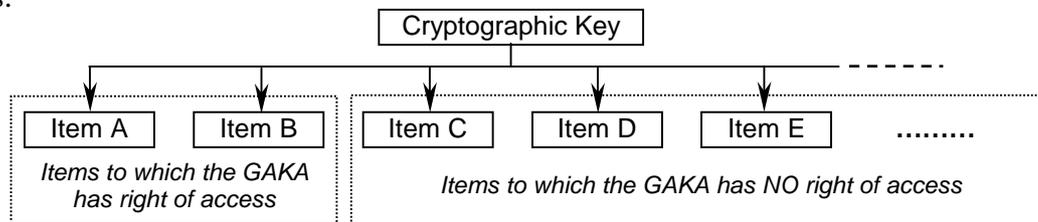
3. In order to understand the implications of the GAK provisions in the RIP Bill it is necessary to understand how modern cryptography works and this is outlined in Annex A. Since Public Key Cryptography (PKC) is now widely used in providing message secrecy, its characteristics have important consequences when considering government access to keys.
4. Firstly, anyone who is using PKC for message secrecy must keep their private key completely secret. If anyone else obtains a copy of a key, the key owner can no longer be certain of the security of the information protected by it. Moreover, revealing the key will also mean that all past messages protected with this key are no longer secure. Hence, once a key has been revealed to others, the owner has lost control of security and can no longer be sure that their messages are protected.
5. A second important feature of PKC is that the key used to send secret messages belongs to the message recipient, not the originator. Hence when a suspected criminal sends a message to a law abiding citizen it will be the latter's key that is needed to read the message and this means there will be many occasions when the GAK provisions will be used to obtain the keys of citizens who are not themselves under suspicion. It is important to bear this in mind in reading the remainder of this paper.

Protecting Keys

6. The extent to which a cryptographic key needs to be protected is determined by the consequence of its revelation and this in turn depends on the volume and the nature of the information which the key protects. If the protected information is of little value, for example a minor electronic purchase, it makes no sense to spend large amounts of money to defend the key that protects this. But if the key is being used to defend something of high value then the key owner will need to protect the key to a much greater extent. There are two important principles here:

- The extent of the protection that a key requires is determined by the extent and the nature of the information it protects.
- The information owner – the person (or organisation) who will suffer the consequences of unwanted revelation – must be in a position to decide how well a key needs to be protected.

7. A key obtained by a GAKA will often protect both information that the GAKA is legally authorised to see and other information which the GAKA has no right of access. This is illustrated in the following diagram which shows a single key protecting many different data items.



8. It is worth pointing out that the use of a single key to protect many different data items is a bad thing to do, especially so if these are of very different character and value. The right approach is to have a number of different keys so that only limited damage results if one becomes revealed. For example, if separate keys are used for protecting financial and medical information, a key seizure by the authorities looking for financial irregularities cannot also create the increased risks to medical data. But the way cryptographic products are being designed at the moment encourages users to rely on single keys. Worse still, the UK government is itself advocating a ‘one key protects all’ philosophy by promoting the use of multi-purpose smart cards where a single security mechanism protects many disparate data items. While, therefore, the ‘one key protects all’ principle is a poor one, it is the situation that the GAK provisions will have to meet.

9. While a key remains solely under the control of the information owner they are in a position to ensure that its protection is appropriate in the light of the consequence of its revelation. But once a key has to be handed to a GAKA the question arises of how well the GAKA should protect it.

10. This raises a difficulty since GAKA do not know the sensitivity of the information protected by the key and this makes it impossible for them to judge how much protection is needed. Some might argue that if a GAKA has secured a right of access, they will have an idea of the information involved and this will hence allow them to assess the level of protection needed.

11. But it will often be the case that seized keys will protect other information to which GAKA have no right of access. In such situations GAKA cannot determine the consequences of the key revelation since they do not know, and have no right to know, all of the information that keys protect. Moreover, the consequences of key revelation fall on key owners, not on GAKA, and this means that they should be able to ensure that their keys are adequately

protected. In principle, therefore, before people hand over their keys, they must be confident that GAKA will protect these to a standard that is sufficient to protect their interests.

12. This presents a difficulty since it is hardly going to be possible for a person served with a decryption warrant to specify how well the GAKA has to protect the key. If this were possible a suspect could avoid handing over their key simply by setting impossible targets. But, bearing in mind that honest people will often be asked to hand over keys, it would be grossly unjust if GAKA did not meet their needs for key protection.

13. As a result there is a difficulty in deciding how well the keys obtained by GAKA should be protected. This cannot be determined by GAKA since they would then be making a judgement that they are in no position to make. On the other hand if the level of protection GAKA are to provide is set by the key owner – as it should be in principle – then anyone who wished to avoid key seizure would simply set impossible demands.

14. The fairest way of resolving this impasse is for Parliament, in enacting the RIP Bill, to decide on the extent to which GAKA will have to protect the keys to which the Bill will provide access. Hence:

in enacting the RIP Bill Parliament must decide on the extent of the protection that GAKA must provide for keys to which they obtain access under its provisions.

What Protection Standards Should Parliament Set?

15. In setting the standards for the protection of cryptographic keys, Parliament will need to bear in mind that many of the keys involved will be owned by people who are not suspected of wrongdoing. Moreover GAKA may handle many keys and while the consequences of revelation of some of these may not be severe, there will undoubtedly be many keys which could have very serious consequences for their owners if revealed or stolen. For the most part people and organisations only use cryptography when information protection really matters and this means that even ‘routine’ keys deserve a high level of protection. It would be unjust in the extreme if Parliament were to pass a law requiring UK citizens to hand over their keys to GAKA that were unable to protect them.

16. How serious could the loss of a key be? For some it will be life threatening.

17. As a practical example consider the position of an exiled politician in the UK who has been democratically elected in their own country but then ousted by an illegal regime which is known to seek out and kill those overseas who are working to restore democracy. The inadvertent or deliberate revelation of the messages that such an exiled politician exchanges with their ‘underground’ colleagues in their own country would not only put their own life at risk but would certainly create immediate and extreme risks for all those with whom this politician has been communicating. This is not a theoretical possibility, it is a real example of exactly the sort of situation in which cryptography is now being used. While the consequences of revelation will not often be as severe as this, it is certain that some keys obtained by GAKA will be such that their revelation will put lives at risk.

18. It is also worth noting that such risks could spread quite widely. An innocuous key seizure in pursuit of a social security anomaly for a dissident, followed by a leak of their whereabouts to a foreign power could result in terrorist action that not only puts the dissident at risk but also endangers the public and members of the police and security forces if an attack results.

19. The consequences of key revelation could also be financial. For example a company may use a cryptographic key to protect its most important trade secrets and many millions of pounds will be at stake if the key is revealed and vital proprietary information becomes public as a result. Such a company would probably go to extreme lengths to protect such a key and any GAKA that seized it would need to provide equivalent or superior protection. Hence if

GAKA protection standards were much lower than those used in industry, an unscrupulous competitor could obtain a key by forcing its revelation to a GAKA and then penetrating the GAKA's protection rather than that of the company itself. Moreover, since a GAKA may have many valuable keys, they will inevitably be a highly attractive target for industrial espionage.

20. To avoid such situations all GAKA will have to protect keys to the highest standards used throughout industry for the most sensitive proprietary information. In fact, even higher standards will be necessary since GAKA may have many such keys.

21. From these examples it can be seen that the revelation of keys while in the possession of GAKA could be extremely serious and even life threatening. And because GAKA have no right to know whether a key is of low or high value they will have to treat all potential key losses as very serious and hence implement the best available protection measures.

22. These considerations lead to the conclusion that Parliament would be undermining the safety and security of UK citizens and companies if it does not set the highest possible standards for the protection of the keys obtained under these GAK provisions.

23. In fact the standards needed are well understood within government since cryptography is widely used for the protection of diplomatic, military and intelligence information. Moreover, since the threats faced by UK agents within hostile foreign countries closely match those of political exiles discussed earlier, the levels of key protection needed to meet such requirements are also well known.

24. That the RIP Bill contains no safeguards in these respects is a surprising and serious omission.

What Sort of Standards Will Be Needed?

25. The UK government experience in the use of cryptography means that there are well developed policies and standards covering such activities. Cryptographic keys are among the most highly protected information items within government and in the light of earlier arguments it is clearly important that the standards that the government uses for its own keys should be extended to provide the same levels of protection for keys that GAKA obtain under the powers in the RIP Bill. The following paragraphs give an indication of the measures that all GAKA will need to implement.

Security Policies

26. Firstly all GAKA will need to develop detailed security policies setting out the full details of the organisational, personnel, procedural and technical measures that they will implement to protect key material obtained under the provisions for GAK.

27. Experience shows that the development of such policies is a highly skilled and specialist task that will either require GAKA to recruit the necessary specialists or to secure the financial resources needed to employ them under contract. In practice it may be less costly to develop a single central security policy to cover all GAKA but this will be enormously difficult because of the substantial differences that exist from one GAKA to the next. For example, while both GCHQ and MOD have considerable experience in key handling, many other GAKA will have to start from scratch and this means one central policy may well be more expensive to implement than the alternative of allowing each GAKA to develop its own approach.

Procedures

28. Each GAKA will need a set of detailed procedures that are to be followed in order to meet the policies it has developed for the handling of GAK obtained keys. This will include detailed descriptions of all the people involved, the processes they will use, the facilities

involved and how these will be operated in such a way that the security of keys is maintained. This will cover the detailed recording of every single action taken with a key and fully secure computer logs in a form suitable for internal auditing and external inspection (discussed later).

Personnel

29. The handling of cryptographic key material requires considerable knowledge and skill and every person in government given such a role has to go through a training course. Every GAKA will have to have an appropriate number of staff trained to handle cryptographic keys and to manage the procedural and technical mechanisms involved in obtaining, storing, using, transferring and destroying keys.

Technical Measures

30. The government has well developed standards for the security of computer systems that handle cryptographic keys. These standards are known as the Information Technology Security Evaluation Criteria (ITSEC) and they have now developed to provide common standards agreed between the US and Europe for the assurance of the security properties of computer systems and products. These 'Common Criteria' are set out in an extensive set of publications available at the UK ITSEC web site (<http://www.itsec.gov.uk/>).

31. In order to set the level of protection required from a key handling computer system it is necessary to know what the threats to these keys are and the consequences of their loss. In general cryptographic keys within government are given a high degree of protection and it would be unreasonable to do less than this for keys obtained under the RIP Bill. Indeed, given that lives will certainly be at stake on some occasions, there is a valid argument for saying that the standards required are at the level of the most valued keys in government rather than those applied for keys of lesser value.

32. Typically systems that are designed to handle cryptographic keys have to meet very high standards and will be special computer systems whose cost is tens or even hundreds of times higher than those which most GAKA would normally purchase. While agencies like GCHQ and MOD will already have systems that meet such standards, other GAKA will not and they will have to find the financial resources needed to purchase and run these systems. Even agencies such as GCHQ and MOD will have to buy new systems since there will need to be rigorous separation of government owned keys and those seized under the provisions in RIP.

33. If the computer systems are networked in any way the transmission of keys will have to be well protected in transmission using high grade cryptography. There is also the threat of electronic eavesdropping and this will mean that the facilities used for handling keys may have to be operated in screened rooms that prevent any information leakage. And, of course, all such facilities will have to be very well guarded physically.

Audit and Inspection

34. Since the protection measures put in place by GAKA do not protect information that they own but rather that owned by those whose keys have been seized, it will be necessary to ensure that all GAK agencies meet the standards set for handling keys before they are allowed to use the GAK powers within the RIP Bill. It will also be necessary to inspect the GAKA on a regular basis and to have the means to obtain independent reports when things go wrong. There is now ample evidence in both the BSE crisis and in the Shipman murder trial that auditing and inspection are vital if standards of public safety and security are to be maintained. These lessons need to be learnt and this will mean that all GAKA (including the Intelligence Agencies) will need to be subject to a rigorous independent inspection to ensure that the safety and security interests of those who are forced to hand over their keys are fully respected.

35. Although GCHQ is responsible for setting the standards for the handling of cryptographic key material in government, they could not be involved in this inspection operation since they are a GAKA themselves. Moreover GCHQ is an Intelligence Agency and many will take the view that they would be inclined to set the standards below those required so that they could themselves exploit any weaknesses in the protection of keys that would result.

36. Public confidence in the operation of the GAK provisions will therefore require an independent inspectorate reporting to Parliament in order to ensure that the protection of keys by GAKA will guarantee the safety, security and privacy of the key owners involved.

The Costs

37. The costs of providing for the adequate protection of seized key material in all the GAKA will be very high. Without looking in some detail at each agency involved it is impossible to know what these will be but experience of the cost of the cryptographic key handling in GCHQ and in MOD suggests that the extension of such mechanisms for all GAKA will result in a very large cost to the UK taxpayer. There is not even the slightest doubt that the costs involved will be counted in hundreds of millions of pounds.

38. The need to protect keys seized under the provisions set out in the RIP Bill is clearly understood within government and this makes it remarkable that the Bill omits any coverage of such requirements. The UK civil service certainly has the corporate experience to know that these costs will be substantial since a number of agencies such as MOD and GCHQ have had to implement the procedural, technical and operational measures that this requires.

The Dangers

39. Compared with conventional computer based data handling operations, the costs involved in systems that meet the security levels needed for handling keys are typically 100 times greater. The costs of such systems will put an enormous strain on GAKA budgets, many of which are already stretched to breaking point, and this will create great pressures to cut corners, for example, by using untrained staff, lax procedures and insecure 'commodity' computer systems. In consequence there is a real danger that the protection needed will not be available with the result that UK citizens and companies whose keys are seized will face seriously increased risks.

40. The financial pressures placed on government and public authorities by legislation for which the financial implications have been either hidden or not fully appreciated are very well known. Police and local authorities are used to central government imposing duties while leaving others to pick up the bill. The consequences are very often higher bills for council tax payers, forced economies in other important areas and all round reductions in the quality and level of service that hard pressed authorities are able to offer the public.

41. While police forces may see GAK provisions as in their interests because they offer an additional weapon in their crime fighting arsenal, they would do well to look carefully at the economies they will be forced to implement elsewhere in order to make room for the very high costs involved in setting up and operating GAK capabilities.

42. Parliament should be very careful before imposing these additional burdens on government and public authorities and hence on UK taxpayers. It will be important to understand what these costs are and how they will be met since if this is not done it is certain that other important duties will suffer.

43. There is no doubt that the costs involved in implementing the GAK provisions will be large; certainly large enough to suggest that Parliament should seek a clear indication from the government of their scale and a cost/benefit analysis to show that the measures are truly justified. Hence:

before enacting the GAK provisions within the RIP Bill, Parliament should seek a full cost benefit analysis of the proposals and full details of the likely cost to UK taxpayers of their effective implementation.

Are These GAK Provisions Really Needed?

44. It is worth noting that the government has provided no significant evidence to show that the measures it proposes for GAK are necessary. It has given some statistics about existing interceptions and implied that the continued success of such methods will be put at risk if the GAK provisions are not enacted. But the statistics provided are very limited and totally lacking in any detail and this has caused many observers to cast doubt on their reliability. Moreover, the inference that interception will be undermined by the wider encryption use is itself a prediction for which the government has provided no significant evidence. It is also being assumed that the proposed GAK provisions will solve this problem if it arises, but this is arguable since many believe that the result will simply be the rapid development of cryptographic products that are specifically designed to circumvent these provisions. Indeed, there is good reason to believe that design work has already started.

45. Further evidence of the lack of real need for GAK legislation is provided by the fact that no other country in the world is taking such action although a number have considered this and thought better of it. Germany has gone even further by making a public statement that the use of cryptography by criminals does not pose a current threat to law enforcement. The German government position is that of keeping the situation under review and being prepared to act if a problem develops. It is hard to believe that the UK has a problem that Germany clearly does not have and this suggests that UK government action on GAK is premature and based more on fear and ignorance rather than on careful analysis of the real need.

Conclusions

46. In respect of provisions for access to encrypted material, the UK government could have taken any one of three paths:

1. It could have done nothing but indicated an intention to act if a problem develops.
2. It could have sought powers for decryption orders that require the decryption of specific messages without requiring access to keys.
3. It could implement, as it proposes, decryption orders giving access to keys.

47. There are strong arguments for the first of these alternatives since being the first government in the world to take action on GAK carries a big risk that the legislation will not have the intended result. Other governments are aware of these issues and many have consciously decided that inaction is the most sensible approach at the moment.

48. Option 2 has not been considered in cost terms in this paper but decryption orders that do not require keys to be handed over are far less risky for those on whom they are served since only a small number of the items protected by the keys in question have to be revealed. This means that the keys themselves are not put at risk and because they are not handed over and this in turn means that the government is not faced with the huge costs of protecting them while in the possession of GAKA. Decrypted information will still need protection but this is on a completely different scale and the costs involved will hence be much lower.

49. In choosing option 3 the government has chosen the most difficult and challenging of the paths that it could take. And in making these proposals to Parliament it has failed in a number of major respects:

- It has failed to justify the need for access to keys, especially so in the light of the policies of other governments faced with the same issues.

- It has failed to set out provisions within the RIP Bill to ensure that agencies authorised to demand keys will implement the necessary policy, procedural, technical and operational measures needed to protect the keys on which the safety and security of their owners depend.
- It has failed to provide Parliament with any cost benefit analysis for these proposals and failed also to give any indication of the scale of the burden on UK taxpayers if they are to be safely and effectively implemented.

50. These are serious omissions which need to be considered very carefully by all members of Parliament before they consider voting for this Bill in its current form. If they pass the Bill while these weaknesses remain they will be putting the safety and security of UK citizens and companies at increased risk without any demonstrable need to do so while at the same time placing a possibly enormous burden on UK taxpayers.

51. In practice these proposals are a continuation of earlier, discredited attempts to introduce key escrow [see Ref 1]. Parliament would be well advised to reject them outright or at very least reject them until the government can make a sound case for them based on a proper cost/benefit analysis and a proper assessment of their costs.

The Author

52. The author worked in the Ministry of Defence (MOD) from 1964 to 1995, specialising from 1978 onwards in all aspects of the safety and security of computer based systems. From 1980 to 1988 he led the UK's primary research and development programme for the implementation of secure information systems within government.

53. From 1988 to 1995 he was Director of Strategic Electronic Communications within MOD where one of his responsibilities was the acquisition of defence cryptographic systems including those involved in the management and distribution of cryptographic key material.

54. In 1995 he became Deputy Director of the NATO SHAPE Technical Centre in the Hague where he held responsibility for NATO research in information security in support of NATO forces deployed in Europe. For three years he was Chairman of the NATO Committee responsible for setting the future standards to be used in secure communications and information systems within NATO.

55. Since 1996 he has worked for a number of companies and for the European Commission on many aspects of information security. He is the Technical Policy Advisor to Cyber-Rights and Cyber-Liberties (UK) and a member of the Advisory Council of the Foundation for Information Policy Research.

Acknowledgements

56. The author would like to acknowledge the valuable comments made by Ross Anderson and Nicholas Bohm in the drafting of this paper.

References

[Ref 1] *Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, and Bruce Schneier. The Risks of Key Recovery, Key Escrow and Trusted Third Party Encryption – a Report by an Ad Hoc Group of Cryptographers and Computer Scientists, Digital Issues no. 3, June 1998.*

Annex A – An Outline of How Cryptography Works

1. Cryptography is a technique that allows information items to be kept secret except among those who have special keys to unlock them. A reasonable analogy for conventional cryptography is a small lockable safe-box which is used by a group of people, all of whom have copies of its key. To send a secret it is placed in the box, which is then locked and sent to the recipient who can then use their key to open the box and read the message. Conventional “Secret Key” cryptography works in the same way – all those who want to exchange secret messages have copies of a secret key. A message sender uses their key to scramble the message before sending it to recipients who then use their copies of this key to unscramble and read the message. The same principles can also be used to protect information stored on a computer.

2. Public key cryptography works in a different way – ‘PKC safe-boxes’ work with pairs of keys, one of which closes a box and the other of which opens it. Each pair of keys is unique and when a box is closed with one of the two keys in a pair it can only be opened with the other key of this pair. And all boxes are delivered with a mechanism that allows owners to make their own unique key pairs. When a person wants to be able to receive secret messages they generate their key pair and give copies of one of the two keys to all of their friends (this is called the public key). They keep the other key secret (this is called the private key) – it is vital that they never, ever reveal this key to anyone. To send them a secret message their friends put this in a ‘PKC safe-box’ and then close this with the recipient’s public key and send it to them. Since the recipient has the only key that can now open the box, only they can recover and read the original message – not even the originator of the message can open the box once it has been closed in this way.

3. ‘PKC safe-boxes’ can also be used in another way. If a person puts a message in a box and closes it with their private key, anyone who finds that they can open this box with a public key knows that whoever owns this public key must have closed the box (since only they have a key that can close the box in such a way that this particular public key will open it). In effect the box acts like the signature of its owner. In practice ‘digital signatures’ are rather more complex but this is the principle on which they are based. Thus, in addition to providing message secrecy, keys can also provide digital signatures but this too depends on keeping the private key secret because copies can be used to forge the owner’s digital signature. This is why the RIP Bill does not allow access to keys that are used only for signature purposes.