ELSEVIER

Journal of Strategic Information Systems 11 (2002) 31–58

Strategic Information Systems

www.elsevier.com/locate/jsis

The regulation of electronic commerce: learning from the UK's RIP act

Ian Hosein[1,*], Edgar A. Whitley[2]

Department of Information Systems, London School of Economics and Political Science, Houghton Street, London WC2A 2AE, UK

Received 2 October 2000; accepted 24 August 2001

Abstract

National governments have a legitimate rôle to play in the development of national strategies to support electronic commerce. It is not always clear, however, what any electronic commerce legislation should incorporate or how regulation of electronic commerce should be implemented. This paper explores the strategic issues that underlie national electronic commerce strategies by following the passage of a particular piece of legislation (the UK's Regulation of Investigatory Powers Act, 2000) through Parliament. In identifying some of the arising strains with the interests of industry and civil society, this paper will discuss some of the legal, technological, economic, and political issues that may arise in other countries as they consider the policy habitat of electronic commerce.

Keywords: Regulation; Electronic commerce; RIP act; Cryptography; Public policy; Technology policy; Technology

1. Introduction

Electronic commerce is perceived as an important element of most developed economies. As a result, most governments are taking an active rôle in determining the regulatory environment surrounding the implementation and development of electronic business. The choice of regulatory intervention depends upon the form of the political economy in the particular jurisdiction together with perspectives on how and why regulation should be implemented for this form of economic activity.

* Corresponding author.
E-mail addresses: i.hosein@lse.ac.uk (I. Hosein), e.a.whitley@lse.ac.uk (E.A. Whitley).
[1] Web page: http://is.lse.ac.uk/staff/hosein.
[2] Web page: http://is.lse.ac.uk/staff/whitley.

0963-8687/02/$ - see front matter
PII: S0963-8687(01)00059-2

This paper seeks to explore the complexity of developing a regulatory environment or habitat (Hood, 1994) for electronic commerce. It does this by focussing on a particular piece of legislation from the UK, the Regulation of Investigatory Powers (RIP) Bill that received the Royal Assent on July 28th 2000. This can be seen as one of the strategic measures undertaken by the British government in an effort to provide a level playing field for electronic commerce in the UK.

The Bill was one of the most highly contested pieces of legislation to be placed before the British Parliament in recent years. From the outset, the government argued that it was well thought out, having been the result of detailed engagement with 'serious commentators' (Clarke, 2000b). However, the business community, and privacy advocates, undertook a major political activity to try and change the legislation in a number of its key areas, suggesting that despite the best efforts of the government, there were still many viewpoints on the process that hadn't been understood properly or taken into account fully.

The controversy surrounding the introduction of this piece of legislation indicates the inherent complexities surrounding the regulatory habitat (Hood, 1994) for electronic commerce. The Bill highlighted the conflicting requirements of secure communication and access requirements of law enforcement agencies; the problems of legislating in a rapidly changing technological environment; the need to minimise the costs and risks of any proposed legislation; the goal of maintaining the human rights of those affected by the legislation; and doing all this in a global context.

In order to understand these issues the paper draws on theories of regulation. Research on regulation typically seeks to address three main questions: Why is regulation introduced for an area? How is the form of the regulatory intervention determined? How is the process of introducing and implementing the regulation managed? This paper presents the case of the British governments' attempts to arrive at a regulatory regime, and how the strategies shifted due to conflicts and opposition. This is particularly observable within the process of passing the RIP Bill, which is then investigated in detail, through analysis of public discourse and parliamentary Hansard.

Section 2 reviews the traditional arguments for government intervention through regulation and introduces the key issues that any understanding of regulation must address. Some initial responses to these issues are then presented, before reviewing the broader context of policy making on cryptography in the UK. This policy debate led to the RIP Bill and the paper then reviews the decisions made about the research method before describing the Bill in Parliament and the issues it raised. Through a presentation of the Parliamentary debate, the paper highlights those areas of the Bill that were changed and the reasoning behind the changes, together with those aspects that were left unchanged despite protestation. The paper ends with a discussion of the lessons learned about the regulation of electronic commerce from the experience of the RIP Bill.

2. Governments, regulation and electronic commerce

Despite the increasingly global nature of business (Braithwaite and Drahos, 2000), which some see as limiting the rôle and scope of governmental action (Angell, 2000; Beck, 2000), it is still the case that governments play an important rôle in the regulation of

domestic affairs. All businesses are tied to local environments and hence to local legal frameworks, whether they are brick and mortar firms or new organisations undertaking electronic commerce. These legal factors govern all aspects of business, from matters of incorporation and taxation, through mundane issues of the lease or purchase of commercial property, to issues associated with the particularities of electronic commerce.

Even the Internet, often seen as borderless, is susceptible to 'unilateral' action taken by local governments. For example, the Bavarian Court ruling on the content provided by CompuServe (Goldsmith, 2000, p. 142) and the French ruling against Yahoo! banning the sale of offensive memorabilia on its auction sites (Akdeniz, 2001) had impacts far beyond the local jurisdictions 'covered' by the rulings which may give rise to conflict over jurisdictions (Yahoo Inc. Vs. La Ligue Contre Le Racisme et L'Antisemitisme, 2001). Multilateral action, taken by groups such as the G8 (G8, 1997) and the Council of Europe (Council of Europe, 2001) can also affect Internet activities and even infrastructure design.

The notion of government intervention in commercial activities is not new; in the UK it can be traced back to the Tudor and Stuart periods. Regulation has been articulated as serving 'the public interest', especially when traditional market mechanisms are not believed to be working properly. To be credible, however, any form of regulation has to be more effective than the market mechanisms it replaces, as the costs of ensuring compliance can be considerable (Baldwin et al., 1995).

Government intervention as a result of new technology is not new either. Contemporary literature in most disciplines discusses technology as a disruptive force to the status quo. The regulation literature notes that information technologies can change the nature of regulated industries, as in Peltzman (1989) on the sources of pressure for deregulation, being

> …changes in the 'politics' and changes in the 'economics' of the regulated industries. Political change includes such things as shifts in the relative political power of contending groups and changes in the underlying organization and information technologies (p. 108).

Peltzman continues that technology is a disruptive force on regulations ranging from interest-rate regulation (p. 121) to telecommunications regulation (p. 117). Likewise, Hood (1994, p. 11) reports on various theories on the reversals of policy, including the cause of a 'loss of policy habitat' that can be a result of 'structural changes' such as the change of technology.

As a result, applying a regulatory regime to a new domain, such as electronic commerce even with its changing technological environment, may seem natural. Within a specific proposed regime, there are challenges that may arise, and conflicting goals may become apparent.

2.1. Interrogating regulatory intervention

(Baldwin et al., 1995) introduce the following framework for interrogating a new regulatory intervention: Why is regulation introduced for an area? How is the form of the regulatory intervention determined? How is the process of introducing and implementing

the regulation managed? Using this framework, the paper will identify some issues surrounding electronic commerce regulation.

2.1.1. Questioning the need to introduce new regulation

In traditional industries, regulation is often considered for monopolies; to address 'windfall' profits; to manage externalities and information asymmetries; to ensure continuity or availability of service; to control excess competition; for public goods and situations of scarcity and rationing and for circumstances where bargaining power is unevenly distributed or for other social policy aims (Baldwin et al., 1995).

Regulation is also considered necessary in order to be consistent with existing statutes and other regulatory regimes, especially in the light of technological changes. This can take the form of introducing regulation for the first time, for example, the introduction of the 1984 Data Protection Act; or as is common in Europe, updating and introducing new legislation as a consequence of other Acts and international agreements. For example, the Council of the European Union 1995 Directive on data protection (European Union, 1995) required implementing new harmonized regulations in member countries on data protection and therefore the 1984 Act was superseded by the 1998 Data Protection Act. Furthermore, such previous regulations are often updated, in order to consider varying technological environments (European Union, 1997) or due to changes in the technological environment (European Union, 2000). Therefore, new regulation is introduced to maintain consistency with existing regimes, and to cater for new technological developments.

2.1.2. Determining the form of new regulation

There are a variety of regulatory interventions that are possible, with varying levels of control exerted. Excluding the *laissez faire* ideal, at one end of an interventionary-spectrum is self regulation, where the government delegates the task of regulation to the industry itself. This is particularly common in media regulation where governments do not wish to be seen to be controlling the media; and is effectively the policy in the US with regards to privacy legislation because of fears of hurting the market with onerous legislation (Armey, 2001; Hahn, 2001).

At the other end is regulation through statute and the creation of regulatory bodies. In the UK, regulation is often enforced by specially created regulatory offices, such as OFWAT for the water industry (OFWAT, 2000), OFSTED for standards in education (OFSTED, 2000) and OFGEM for gas and electricity supplies (OFGEM, 2000). Between these extremes other forms of intervention also exist, such as voluntary regulation, licensing and co-regulation (Baldwin et al., 1998).

2.1.3. Questioning the process of introduction and implementation

The means by which regulation is introduced varies between political systems. In the US, the emphasis is on due process and open hearings, whereas in the UK a system of closed negotiation and confidential hearings is preferred. In the light of the recent controversies surrounding BSE related health scares (Seguin, 2000), there are proposals for reform to the British approach. The British approach results in a cheaper and quicker

process than the US, although there is a risk of haphazard decision making as the various interests are heard together, rather than through separate hearings (Baldwin et al., 1995).

2.2. Initial considerations

When these questions are addressed to the environment of electronic transactions, certain issues become apparent immediately. For example, one of the factors influencing the need for new regulation is to maintain the traditional powers of the state (Hosein, 2001). When new regulation is applied for electronic commerce, there is a need to ensure that such interests are addressed within the new regulatory habitat.

Although other forms of intervention such as voluntary regulation, licensing and co-regulation were considered in the UK, they were deemed inadequate due to the nature of the market considered and the effectiveness in meeting the Government's goals. When the Department of Trade and Industry (DTI) was directly responsible for the electronic commerce strategy, and statutory intervention, it considered establishing licensing regimes. As the responsibility shifted to the Home Office, a different form of intervention was settled upon with the introduction of the RIP Bill. That is, a statutory intervention effecting obligations on the individual and industry was selected as the only effective way of meeting the interests of the British Government.

As a result, we notice that the selection of the ideal body for managing the British electronic commerce policy was in itself a challenge. Responsibilities shifted between economy-minded institutions and executive institutions: in the UK it was from the DTI, to the Cabinet Office, and ultimately the Home Office. In common with many areas that are to be regulated, electronic commerce does not fall naturally within the scope of any one department and so political choices need to be made as to who will take ownership of the regulations and see them through parliament and beyond (Baldwin and Cave, 1999). This is in direct contrast to the US where policy on cryptography began in national security institutions, and moved gradually to those relating to commerce.

The choice of body and the nature of intervention also affects the process. While the US has an open process of testimonies to Congress and public media lobbying, the British discourse was remarkably different. When the DTI was responsible for the strategy, the process involved public consultation documents and submissions. After this did not result in the government's desired outcome, the Home Office assumed responsibility, but in so doing limited much of the contentious discussion by releasing the RIP Bill for consideration in Parliament without significant prior consultation on the issue of encryption. As a result, the greatest proportion of the debate occurred within the Parliament (between parliamentarians rather than within the public domain), and surprisingly more so within the House of Lords, an institution that is often felt to be disconnected with the public. This resulted, again surprisingly, in a great deal of last minute amendments to settle some of the interests of industry and advocates.

2.3. Beyond the framework: further considerations

A further issue that is looming behind all of these considerations is globalisation. The global nature of business also means that governments must act with an appreciation that any actions they take may have effects outside their borders. While this is not necessarily

new (and has often been a consideration in taxation policy, or international judgements (Hague Conference On Private International Law, 1999)), it is argued below that the electronic commerce infrastructure may enable cross-border technical and organisational designs and implementations.

In particular, if governments make the environment less amenable to Internet-based companies then they can relocate, with greater ease than traditional companies, to other locations outside that particular jurisdiction, with knock-on effects for the local economy (Angell, 2000). These 'knock-on effects' will affect the varying interests of the state, including economic growth and taxation, as well as surveillance capabilities.

To conclude, introducing a new regulation involves many strategic issues, and this may be particularly the case within changing technological environments, and within industries, such as electronic commerce, that captivate actors with the great potential and excitement. The decision of who intervenes may shift, the process of policy development is thus affected and affects the selection of the mode of intervention, and the predominance and conflicts of interests arise and await settlement. This all occurs within an industry that can shift to other jurisdictions, and with technology that can, and often does, alter the policy environment and transforms traditional powers and institutions (Hosein, 2001).

In Section 3, the broader context of policies on cryptography are introduced. The section reviews the ways in which policy discussion on cryptography was undertaken, a discussion that resulted in the RIP Bill.

3. From the beginning: policies on cryptography

Electronic commerce policy and cryptography policy within the UK have been almost inseparable, even though they have ended up being *officially* addressed in distinct pieces of legislation. The regulation of modern cryptography dates back to the Cold War, and multilateral agreements to restrict the export and use of cryptography due to national security concerns (Wallace and Mangan, 1997, p. 42; Heinz, 1991). These concerns of national security transformed into law enforcement concerns as communications technologies became more widespread and advanced: individuals, and not just foreign governments, could use cryptography to encrypt files and communications, which could only be decrypted using keys in the possession of the individual, and this would interfere with traditional powers of the state, and existing statute.

While open discussion of cryptography policy in the US began in the late 1980s and early 1990s before the promise of electronic commerce, the UK began its debate about its regulatory intents much later. This timing has interesting discourse implications. The US, for many years framed cryptography regulation with respect to national security concerns and was forced eventually to consider it under law enforcement concerns, and in the mid-1990s the concerns of electronic commerce joined the fray. On the other hand, because the UK addressed the issue after the advent of electronic commerce, the British governments were forced to address cryptography and its various implications in tandem with electronic commerce. That is, cryptography, as is articulated below, is considered essential to secure electronic commerce, so any policies on electronic commerce necessarily affect existing cryptography policies, as the US realised over time; while the UK (and other contemporary

national policies) noticed that discussion of cryptography policy could not occur without discussion of electronic commerce and conducted the discourse accordingly.

In 1996, the DTI announced its *Regulatory Intent Concerning Use Of Encryption On Public Networks* (DTI, 1996). Although there had been previous speeches and limited discussion on the topic, this was the first active statement of intent from the government. The regulatory intent was 'to facilitate the development of electronic commerce by the introduction of measures which recognise the growing demand for encryption services to safeguard the integrity and confidentiality of electronic information transmitted on public telecommunications networks'.

The government proposed the creation of Trusted Third Parties as key elements in the electronic commerce infrastructure. These third parties had a secondary rôle, however: they were required to retain copies of decryption keys to 'preserve the ability of the intelligence and law enforcement agencies to fight serious crime and terrorism by establishing procedures for disclosure to them of encryption keys, under safeguards similar to those which already exist for warranted interception under the Interception of Communications Act' (DTI, 1997).

This intention was developed into a consultation paper from the DTI in 1997 (DTI, 1997) which outlined the implementation and licensing of these trusted third parties. These parties, deemed by government to be required by electronic commerce, were to fall under a mandatory licensing regime, where the license would only be granted if these third parties stored a copy of all decryption keys of their clients. This depository of keys held by trusted third parties could then be accessed by government law enforcement and national security agencies.

During the resulting debate about the proposals, many organisations pointed out that decryption keys must be kept secure, and having government access to keys through trusted third parties was introducing risks to the security of the system (Abelson et al., 1998), thus conflicting with the government's goal of supporting and developing electronic commerce (Hosein, 1998).

The policy was placed on hold after the consultation process as an election occurred. Even during this election campaign, which resulted in a change of government from Conservative to Labour, cryptography and electronic commerce policy was an issue. In its 1997 election manifesto, the Labour Party had stated:

> The only power we would wish to give to the authorities, in order to pursue a defined legitimate anti-criminal purpose, would be to enable decryption to be demanded under judicial warrant (in the same way that a warrant is required in order to search someone's home).
>
> Attempts to control the use of encryption technology are wrong in principle, unworkable in practice, and damaging to the long-term economic value of the information networks.
>
> Adequate controls can be put in place based around current laws covering search and seizure and the disclosure of information. It is not necessary to criminalise a large section of the network-using public to control the activities of a very small minority of law-breakers. (Labour Party, 1997).

Perhaps unsurprisingly despite the 'New' Labour label, many of the new government's

policies were in fact continuations of policy processes initiated by the previous Conservative government.

Over the next two years the government responded to business concerns and criticisms of the previous *mandatory* approach to licensing trusted third parties (DTI, 1998 sec 14). It proposed instead a *voluntary* licensing scheme, where licensing was contingent on the third party storing a copy of the decryption key of an individual, thus upholding the principle of government access to keys and through statute provides for lawful access to keys:

> (In response to these concerns) the Government intends to introduce legislation to enable law enforcement agencies to obtain a warrant for lawful access to information necessary to decrypt the content of communications or stored data (in effect, the encryption key). (DTI, 1998, sec 14)

This policy was further developed in another consultation process from the DTI (1999a). This report also included a technical differentiation, which was an attempt to differentiate between the interests of secure electronic commerce and government access to keys for maintaining a safe society. This technical differentiation involved the acknowledgement that digital signature keys with integrity/authentication properties (assumed to be under licensed Certification Authorities) were separate from decryption keys with associated confidentiality properties (assumed to be under a trusted third party regime). These Certification Authorities would be used to provide confirmation of the identity/authenticity of individuals and transactions and verify non-repudiation; essentially electronic commerce concerns. The provision of these authentication services was separated from the ability to decrypt encoded messages, which would be handled by the trusted third parties and their key-depositories:

> The Government is committed to a clear policy differentiation between electronic signatures and encryption. This reflects the valid concerns expressed by industry during the consultation process launched by the previous administration, and recognises the different commercial applications of these services and the different challenges they pose to Government policy (sec 35).

The response to this second consultation document was still one of general concern, as the DTI (1999b) reported:

> Many people repeated the view that the whole issue of lawful access should be decoupled from the measures to build confidence in electronic commerce, and would be better dealt with in a separate Bill, possibly after the forthcoming Home Office review of the Interception of Communications Act 1985. Confidence-building measures were thought to be more urgent, whilst lawful access measures were seen as: (a) likely to cause delay, and (b) having the potential to reduce confidence in the UK as a good place to base an electronic commerce service or business (sec 5).

During this period, the Prime Minister, through the Cabinet Office, commissioned a report from the Performance and Innovation Unit (PIU), entitled Encryption and Law

Enforcement (PIU, 1999). In a foreword written by Prime Minister Tony Blair, he outlined clearly the dual-interests of government:

> I am determined to ensure that the UK provides the best environment in the world for electronic business. …But I am equally determined to ensure that the UK remains a safe and free country in which to live and work. The rise of encryption technologies threatens to bring the achievement of these two objectives into conflict. (PIU, 1999 foreword).

Continuing this strain of objectives and interests, the PIU report outlines the importance of encryption technologies to electronic commerce (chapter 3), but also the importance of access to law enforcement (chapter 4). The report acknowledges that the past measures of government were unlikely to allow access to the communications and stored data of criminals who would operate outside of the voluntary regimes (p. 12), and doubts the commercial success of the trusted-third party key depository service (p. 13). As a new approach, the report advocated working with industry to find a solution, and to support the idea of legislation on lawful access to individuals' decryption keys rather than the key depositories (p. 15):

> (t)he task force welcomes the intention to include in the Electronic Commerce Bill provisions to allow lawful access to decryption keys and/or plain text under proper authority. The task force also recommended that further attention should be given in the Bill to placing the onus on the recipient of a disclosure notice to prove to the authorities that the requested keys or plain text are not in his possession, and to state to the best of his knowledge and belief where they are. (p. 15).

What followed from the PIU report and the consultation paper was a phase of flux. During this period, the Home Office began consultation on alterations to the 1985 Interception and Communications Act (Home Office, 1999) dealing with lawful access to communications and traffic data. Additionally, as mentioned in the PIU report, a draft Electronic Commerce Bill was released by the DTI, as presented to Parliament by the Secretary of State for Trade and Industry in July 1999. The most notable part of the bill was the granting of government powers to gain access to keys under a notice (ECB, 1999, Part III). The remainder of the Bill dealt with the legal recognition of digital signatures, and the operation of Certification Authorities. Again this gave rise to controversy and threatened the introduction of the Bill due to problems surrounding a legal audit (Beatson and Eicke, 1999) commissioned by a think-tank, the Foundation for Information Policy Research, and a civil liberties organisation, Justice, stating that the Bill may be in contravention to the European Convention on Human Rights. The variety of arising issues (as in FIPR, 1999) included self-incrimination; the process of handing over keys and uncertainty as to which key was required to be given to law enforcement: would session keys suffice, or would private keys be required? The draft Bill did not recognise any differences amongst keys beyond the granularity level of signature keys and decryption keys, as realised in 1999 despite the issue having been raised during the consultation process (Hosein, 1998).

The most contentious section surrounded the failure to disclose a requested key. If the individual receiving a disclosure order does not disclose the key, a prison sentence may be

imposed. If the key is lost, forgotten, or deleted, the draft Bill requires that proof of this loss is provided by the individual. The result, which the Home Office refuted for most of the length of this process (Home Office, 2000), is that there is a reverse burden of proof: failing to make such a proof, the individual can be given a prison sentence (FIPR, 1999).

The draft Bill also introduced the offence of Tipping-Off, whereby if an individual's key was accessed by government, this individual could not notify anyone of this situation, under penalty of a prison term (Swarbrick, 1999). This is both a commercial concern (corporate officers would not be informed if their communications were, potentially, compromised) and a human rights concern because it constitutes a 'gag-order', and may force an individual to continue using a compromised key.

As a result of the controversy about this Bill, the Queen's Speech in November 1999 introduced the Electronic Communications Bill which was free of issues relating to decryption keys, coupled with a promise that the Home Office would update the Interception of Communications Act, 1985. The British Department of Trade and Industry managed to get onto statute the legal recognition of digital signatures to support electronic commerce (under the Electronic Communications Act 2000), while issues surrounding investigatory powers and access to keys were moved to the Regulation of Investigatory Powers Bill, introduced on February 9th 2000, under the responsibility of the Home Office.

These are summarised in Box 1

March 1996	Regulatory intents on encryption: Creation of Trusted Third Parties involving key escrow proposed
March 1997	Consultation paper on the licensing of trusted third parties
April 1998	Statement on Secure Electronic Commerce: Non-mandatory licensing of third parties who must till escrow keys in order to be licensed
March 1999	Building Confidence In Electronic Commerce: Separation of trusted third parties from certification authorities. Third parties must still escrow keys in order to be licensed
April 1999	PIU report forces abandonment of third party escrow
June 1999	Electronic Commerce Bill introduced: Enabling digital signatures plus government access to keys and tipping-off offense
July 1999	Home Office begins consultation on revising the 1985 Interception of Communications Act
November 1999	Queen's speech introduces the Electronic Communications Act that deals solely with digital signatures. Other issues left for RIP Bill
February 2000	RIP Bill introduced into Parliament

Despite attempting to separate out electronic commerce and lawful access, the government could not escape debate on how the investigatory powers may harm the country's hope for electronic commerce. Various interests and strategies collided throughout the process, ranging from the interests of a secure economy, supporting a growing net economy, maintaining a safe society, the protection of individual rights, to name a few. While many of the concerns raised about Part III of the Draft Electronic Commerce Bill

were almost completely transplanted to the RIP Bill the government managed to separate, in statute at least, the issue of electronic commerce from the issue of lawful access to decryption keys.

The introduction of the RIP Bill to Parliament began a debate about many of the complexities of legislating for a regulatory framework for electronic commerce. Section 4 reviews the research approach used to understand the study the Bill in its passage through parliament.

4. Research approach

Any research process consists of selecting possible data sources, data collection and data analysis. All three stages offer the potential for information overload (Roszak, 1994; Shenk, 1997; Postman, 1992), so a key element of doing research is deciding which resources should be considered and which should be ignored. The choice of which sources to use, which elements to collect and which to analyse is normally informed by the methodological principles underlying the research. This section reviews and justifies the choices made in this research project.

The research reported here takes place within the interpretive tradition (Klein and Myers, 1999) which does not accept that there is a single objective reality which all participants are working towards (Walsham, 1993), but rather that different participants bring different perspectives on the issues which influence their understanding of the situation and their resulting actions. It is also influenced by the literature on regulation (e.g. Baldwin et al., 1995) and ideas found in actor-network theory (Latour, 1999; Law and Hassard, 1998). In particular, from actor-network theory it takes an explicit consideration of the rôle played by non-humans (in this case particularly the encryption algorithms) in human activities (Latour, 1992; Pouloudi and Whitley, 2000). One further influence on the work has been the direct involvement of one of the authors in the opposition to the RIP Bill.

In the UK, as mentioned earlier, decisions about the regulation of electronic commerce have typically been left to government. The consideration of the factors that influence regulation in this context will therefore draw heavily upon governmental debates on this issue. A large amount of information is publically available. One of the key data sources is Hansard. Hansard is the official record of all British parliamentary debates and is available from the Parliament website. The material in Hansard is supplemented by material from British national newspapers (over 450 articles appeared about the RIP Bill during its progress through parliament) and private discussions with those who lobbied for changes to the Bill.

Coupled with the length of the Bill itself, all this information means that it is necessary to have a ‘coordinated series of techniques for reducing the amount of information that requires processing’ (Postman, 1992, p. 84). In order to make the analysis manageable the paper therefore focuses on those particularly contentious elements of the Bill described earlier: Part III dealing with lawful access to keys.

The information from these various sources was combined and a detailed reading of all the key materials was undertaken (cf. Beath and Orlikowski, 1994). Given the large

amount of material available, one would normally expect some form of structured system for indexing the materials. In this case, however, as one of the authors was also involved in the lobbying process and has a deep interest in the processes by which the regulation of electronic commerce takes place, this was not necessary; this detailed knowledge was part of the author's *weltanschauung* and was useful for regular lobbying activities outside the academic context. Steps are in hand, however, to develop a suitable index for this material, to ensure that such detailed access to the material is available over time.

Having identified the relevant materials from Hansard and elsewhere it must be analysed and used to support an argument. One strategy would be to use the authors' understanding of the material to present their review of how the debates about the regulation of electronic commerce proceeded. Such a strategy always carries the risk of the authors' over-interpreting the material and adding their own biases to the material.

To that end, Section 4.1 will be presented with extensive quotations from the relevant debates. This is done to help convey some of the broader contextual issues influencing the debate. In this case, for example, this broader context includes issues of cryptography, human rights, existing statutory powers and protections, surveillance and the protection of society, globalization and changes in technology, costs and risks.

4.1. The key elements of the Part III of the Bill

Part III of the RIP Bill was essentially the same as that which was in the Draft Electronic Commerce Bill 1999. Particularly, the RIP Bill Sections 46 through to 51 (referred to as B46-B51) each addressed particular issues relating to how keys could be accessed, associated offences, and safeguards. Later we will address some of these sections in detail.

Section B46 granted government the power to require disclosure of key through a notice. That is, where protected information has come under the possession of the authorities, and where these authorities believe a particular person on reasonable grounds has the means to make this protected information available by use of a key, and the disclosure of the key is likely to be of value for purposes connected with the exercise or performance by any public authority of any statutory power or statutory duty, and such a disclosure is proportionate to what is being achieved, then the authorities may require its disclosure. Such a disclosure can take place under three requirements:

- in the interests of national security;
- for the purpose of preventing or detecting crime; or
- in the interests of the economic well-being of the UK.

where national security and economic well-being are borrowed terms from other statutory instruments.

Section B47 allows for a situation where the protected information can be made intelligible by the recipient of the notice, and given to the authorities, rather than the key itself. More precisely, the recipient of the notice to disclose the key may use the key to render the

information into an intelligible form and provide the authorities with this information. This can only occur in situations where the authorities did not specify that compliance is measured through only the disclosure of the key.

If an individual fails to comply with the notice, then he is guilty of an offence under B49. An individual fails to comply if he or she has or had possession of the key and claims to no longer have it. The burden of proof is placed upon the individuals, however, to prove that the key was not in their possession after the notice was received, or that it was not reasonably practicable for them to disclose the key. If the individuals fail to prove the above, then they are guilty and may be imprisoned for up to two years.

Another offence is that of tipping-off, as declared in Section B50. That is, a notice can require that the disclosure of the key must be kept secret. Such a requirement can be placed 'in order to maintain the effectiveness of any investigation or of investigatory techniques generally, or in the interests of the safety or well-being of any person' (B50.2). Failing to comply with this requirement may result in a five year prison term.

5. The Bill in Parliament

The Regulation of Investigatory Powers Bill was introduced to the House of Commons at 3.31 p.m. on February 9th 2000 (Hansard, 2000a Column 250) and brought back for its second reading by Mr Jack Straw, the Secretary of State for the Home Office, at 3.35 p.m. on March 6th 2000 (Hansard, 2000b Column 767).

The Bill continued on to the House of Commons Committee, where it was discussed with amendments from March 14th 2000 to April 6th 2000. It then proceeded to Report Stage and Third Reading on May 8th 2000 where it was amended further and sent to the House of Lords for consideration. The amendments considered at the House of Commons stage, a process that lasted a span of four months, were minimal.

First, the form of the notice for key disclosure was expanded. Second, additional constraints were added to the process of when the authorities request key disclosure (rather than the plaintext). That is, law enforcement agencies could only request key-only disclosure if they did not believe that the true plaintext would be given by the individual. Additional amendments were made on the secrecy requirements within Section B50, and some more specific statements on the defence for tipping-off.

The Bill was introduced to the House of Lords by Lord Bassam, the Home Office Minister, first on May 9th 2000, with a second reading on May 25th 2000. Part III was discussed specifically in Committee Stage on June 28th 2000, where a significant debate occurred, and the Home Office Minister introduced amendments at the last hour. Part III was then discussed in Report Stage on July 13th 2000, when further amendments were introduced. The Third Reading occurred in the House of Lords on July 19th 2000, after which the Bill was returned to the House of Commons for consideration of the Lords Amendments on July 26th 2000. The amendments were commended by the Home Office Minister in the House of Commons and the Bill received Royal Assent on July 28th 2000.

Box 2 summarises the various stages the Bill went through in Parliament.

House of Commons
RIP Bill Introduction 9th February 2000
Second Reading 6th March 2000
Committee stage 4th April 2000
Third Reading 8th May 2000

House of Lords
Introduction 9th May 2000
Second reading 25th May 2000

Committee stage
1st Committee Sitting, 2 Sessions (12th June 2000)
2nd Committee Sitting, 3 Sessions (19th June 2000)
(Dealt with other parts of the Bill)
3rd Committee Sitting, 3 Sessions 28th June 2000
Report stage 12th July 2000
Third reading, 2 Sittings 13th July 2000

Commons consideration of Lords amendments 26th July 2000
Royal Assent 28th July 2000
(Adapted from http://www.homeoffice.gov.uk/ripa/ripleg.htm)

5.1. Electronic commerce issues raised by the Bill

The question of secure transactions appears to conflict with the requirements of law enforcement agencies to have access to communications, as enshrined in earlier statute (such as IOCA 1985), and limited by recent statute (the Human Rights Act 1998, which is the national implementation of the European Convention on Human Rights). When the Bill was introduced into Parliament, this point was made by Jack Straw, the Home Office Secretary, who stated that it was an important Bill that represented 'a significant step forward for the protection of human rights in this country'. It sought to update existing law enforcement activities to secure 'a better balance between law enforcement and individual rights', which is seen as an important responsibility of the Government and the Home Office in particular:

> The Bill is intended to allow the law enforcement agencies to maintain their success record against a diverse series of threats including drug trafficking, money laundering, human trafficking, paedophilia, tobacco smuggling and other serious offences (Hansard, 2000b Column 768).

The part of the Bill that has the greatest effect on electronic commerce is Part III that dealt with demands to decrypt data. As Mr Straw acknowledged '(E)ncryption itself is vital to the success of the e-commerce revolution, and helps to prevent certain types of crime, such as fraud on the Internet'. However, he pointed out, it can also be used 'by

criminals to frustrate law enforcement', which 'is happening already, and the problems will increase as the technology becomes more available' (Hansard, 2000b, Column 775) and so a new decryption power is needed to maintain the effectiveness of existing powers. Thus, the Bill proposed to allow an investigating agency that 'has reasonable grounds for believing that a key exists to decrypt lawfully acquired data …to require the decryption of that data" (Hansard, 2000b Column 775). Therefore, in the UK no encrypted data would be beyond the reach of government.

Similar statements were made in the House of Lords, for example, when Lord Bassam, in an attempt to align industry interests with law enforcement interests, asserted:

> Our goal is to make this country the best and safest place in the world in which to carry out e-commerce. I know that industry, too, wants a secure environment in which to operate (Hansard, 2000d 883).

From the reading of Hansard, it becomes apparent that three further issues are clearly implicated in the legislation. The first issue is the business costs associated with any legislation. The second is the implications for human rights. Finally, there is the problem of legislating technology in a rapidly changing environment. Each of these issues will now be discussed in turn, beginning with the conflict between the need for secure electronic commerce and the access requirements of law enforcement agencies.

5.2. Business implications of the act

The requirement that government agencies must have access to encryption keys was particularly provocative. First, there was the practical issue that any secure communications based in the UK would potentially be open to interception by government agencies. Second, the costs of implementing the Bill would have direct effects on the costs of doing business in the UK (ISPA, 2000). Both concerns could encourage companies to move out of the UK, with a further effect on the British economy (BCC, 2000). These costs were explored in the report commissioned by the British Chamber of Commerce.

The BCC commissioned report noted that the interception capability requirements of Part I of the RIP Bill was in itself onerous (the order of £12–£18 million per annum—see Whitley and Hosein, 2001 for more details), and that these costs would be borne, to a large extent, by the Internet service providers and would have a profound effect on their cost structure and hence knock-on effects on their customers. On the issue of lawful access to keys within Part III of the Bill, the BCC report noted that there are further costs associated with the possible key seizure (BCC, 2000, p. 14), which are listed in Box 3

Public disclosure of critical company information
Increased opportunities for industrial espionage
Reduced trust and confidence in company security
Market disadvantage
Customer and client concerns

The BCC report suggests that the potential danger to encrypted, legitimate business information is such that many companies would seriously consider relocating their service

provision outside the UK, to countries like Denmark which have decided against policies which require disclosure of keys (BCC, 2000). The combined cost to the British economy of losses and leakages from all aspects of the Bill was claimed to be as high as £46 billion, a figure hotly disputed by the Home Office (Home Office, 2000; Straw, 2000). Some companies did announce their intentions to move their services off-shore, as covered in (Whitley and Hosein, 2001); however the current status of their intentions a year later are not known to the authors.

5.3. Human rights

The proposed act can also be seen as part of the government's response to the new Human Rights Act. The RIP Bill was presented as a mechanism for the protection of civil liberties. As the Home Office Secretary stated on the Bill's Second Reading in the House of Commons:

> This is an important Bill, and represents a significant step forward for the protection of human rights in this country. Human rights considerations have dominated its drafting. None of the law enforcement activities specified in the Bill is new. What is new is that, for the first time, the use of these techniques will be properly regulated by law and externally supervised. That will serve to ensure that law enforcement and other operations are consistent with the duties imposed on public authorities by the European Convention on Human Rights and by the Human Rights Act 1998 (Hansard, 2000b Column 767).

This point was echoed by Lord Bassam in the debates in the House of Lords:

> I can assure noble Lords that the concept behind the Bill is very simple. It regulates six investigatory powers. Five of the powers are used already and the Bill will ensure that that use is regulated in accordance with the requirements of the European Convention on Human Rights (Hansard, 2000d Column 880).

The fact of the matter is that the British Government is practically obliged to come up with some form of statutory reasoning for the powers of investigation; this is due mostly to the incorporation of the European Convention of Human Rights (ECHR) in to the Human Rights Act 1998 (HRA) which became effective from October 2nd 2000. Because of case law arising from the ECHR (Beatson and Eicke, 1999), if the government intends to breach the human rights of an individual, particularly in this case the right to privacy, it has to have these powers proclaimed in statutory instruments. Otherwise their practices will be considered in contravention to the European Convention and the Human Rights Act, and these powers would be considered illegal, and thus unusable.

Moreover, it was noted later that the Home Office Secretary's statement regarding the 'new powers' was fallacious as his colleague Lord Bassam's quotation later indicates: access to decryption keys is in fact a new power, and thus required renewed scrutiny with respect to the ECHR and the HRA due to self-incrimination and burden of proof issues.

5.4. The technological environment

A third complication arises from the rapidly changing nature of the technological environment for electronic commerce, as the Home Office Minister Lord Bassam noted:

> Although, strictly speaking, the sixth power (in the Bill) is new, it arises only as a response to developments in technology. Technology has the potential to limit considerably the capabilities of law enforcement and other agencies in preventing crime. The (decryption) power in the Bill will go some way towards redressing the balance. (Hansard, 2000d Column 880)

and summarises the main apparent interests of the Bill itself:

> Those are the two objectives of the Bill: that the six powers in question should be used in a way that is compatible with the convention (on human rights) and that they should be available to cope with developments in modern technology (Hansard, 2000d Column 882).

although this is soon reabsorbed in the electronic commerce/law enforcement argument:

> We do not want to see the burgeoning e-commerce market overrun by criminals against whom law enforcement agencies find themselves effectively powerless. So, in driving forward the e-commerce revolution, we need to ensure that law enforcement powers are similarly updated. That is precisely what the Bill does (Hansard, 2000d Column 883).

The problems associated with keeping up with technological changes was nicely illustrated in the Lords debate, where members discussed in some detail, technological fixes based on steganography and alternative uses of encryption (Brown and Gladman, 2000) to bypass the proposed law. Despite awareness and discussion of these practical countermeasures, the Bill was still passed.

6. Changes to the Bill

After a significant number of amendments were marshalled in the House of Commons, very few were actually passed. The situation was similar in the House of Lords, where an even larger number of amendments were raised for discussion at the Committee Stage; however the tactics of the Home Office here were different. Rather than debate and be outvoted, the Home Office Minister introduced new amendments to the Lords:

> Throughout the Bill I have sought to be constructive and to offer constructive opportunities to all to make intelligible and intelligent criticisms. We have invited in all sectors of business. To my knowledge, we have not said, 'No, go away' to anyone. That approach has now been widely acknowledged. Therefore, when the Government are criticised for extensively rewriting the Bill, or for putting forward provisions at the very last moment, it is because we have been listening—as we always said we would—and there is no other time when we can make these changes.

> I am sure that Members of this House will recognise and understand that (Hansard, 2000e, Columns 957–958).

These amendments were significant in changing the language of the Bill. The most significant were the amendments that changed the wording in the Bill of default behaviour from 'disclosure of keys with further expansion on disclosure of plaintext instead', to 'disclosure of protected information with special cases where keys are required'. The result was that keys were not to be accessed lawfully by default. Technically, if keys are accessed, then the keys can be used to decrypt all communications sent to that key and files encrypted to it in the past and the future; which is a power and introduces substantial risks to trust and security (Abelson et al., 1998). Rather, the default was changed to plaintext, that is an individual can hand over the plaintext to only the specific communications that were intercepted or files that were searched, and not to all future and other past communications that may be discovered.

The next significant amendment affected key disclosure (and for that matter, protected information) to meet the interests of industry. The amendment changed the wording of the tipping-off offence to allow for the notification of the senior officer of a corporate body if the key or information protected by an employee within that body was being requested for disclosure.

A further set of amendments allow the individual receiving the notice to use any key to transform the protected information into an intelligible form; and when the disclosure requirement is for keys, again the individual may decide *which* key is to be disclosed. In addition, when a key disclosure is required, it is not necessary for the individual to make disclosure of any keys in addition to those that suffice for the disclosure notice. That is, the individual can hand over all the subkeys that relate to the protected information that the authorities have already gathered, without having to worry about handing over keys that may decrypt other information that is outside of the notice request. If an individual creates a key with *subkeys* for every month, and law enforcement officers arrive asking for the keys to decrypt messages received from September 26–30, the individual can hand over either the subkey for September, or may even choose to hand over the *session* keys for each communication instead. The granularity issue first raised in 1997 by opponents of the government policy (Hosein, 1998), addressed partly with the separation of signature and encryption keys in 1999, was finally raised and addressed adequately to allow for a settlement at this late stage.

The reverse burden of proof is also addressed somewhat within the Government amendments at this stage. Removing the 'it shall be a defence for that person to show', the amendments place the burden on the prosecution to show that a person was in fact in possession of a key at a specific time, and thus willingly failed to comply with the law. With boldface to show additions, strikethroughs to show deletions:

> In proceedings against any person for an offence under this section, *if it is shown that that person was in possession of a key to any protected information at any time before the time of the giving of the section 46 notice, that person shall be taken for the purposes of those proceedings to have continued to be in possession of that key at all subsequent times, unless it is shown*
>
> that the key was not in his possession after the giving of the notice and before the time by which he was required to disclose it;

> The individual shall be taken to have shown that he did not have the key only if the prosecution can raise a reasonable doubt.

This change, to a significant extent, placed the burden of proof on the prosecution rather than the individual having to prove innocence/loss, thus limiting the likelihood of the bill being found in contravention to the ECHR and associated jurisprudence.

These changes are discussed in greater detail later.

6.1. Plaintext versus key

From the earliest days of the Bill, the first mention from Mr Charles Clarke, a Home Office Minister regarding the access to keys issue, states that the key versus plaintext issue is actually a non-issue:

> I wish to emphasise one important point. We envisage that the disclosure of the plain text of protected material, rather than a key, will be sufficient in almost all cases responding to a decryption notice and I expect there to be very few cases where disclosure of the keys themselves will be required (Hansard, 2000b, Column 834).

The reason for not changing the original wording, as he elaborates later, is that 'our bottom line continues to be that we must retain the flexibility in the Bill to request the disclosure of the key itself in exceptional circumstances' (Hansard, 2000c). He continues, '(M)any in industry have no difficulty with the principle of handing over intelligible data when they were required to do so under some lawful authority. However, they have some worries about handing over the keys' (Hansard, 2000c).

However, this explanation did not appease all of the opposition. In continuing to raise concerns, Mr Heald (a Conservative, Opposition MP) stated:

> The Minister's recent concession when he said that he was considering putting a requirement in the Bill that the key should be obtained only in exceptional circumstances will have knock-on effects for section 46 notices. I imagine that he is suggesting that one category of section 46 notices would require the plaintext and a different section 46 notice would require the giving up of the key, but only in exceptional circumstances. …There would need to be a protocol or set of guidelines on how institutions should be approached for either category of section 46 notices (Hansard, 2000c).

At that point, however, the issue was not being entertained. Mr Clarke responded:

> We might consider amending the Bill to allow insistence on producing the key only exceptionally and to state what might be exceptional in the code of practice. We might go further and specify that decisions on what is excepted may be escalated to the highest level, so that the Secretary of State or a chief constable, possibly with the approval of a surveillance commissioner or circuit judge if appropriate, would decide whether a circumstance was exceptional according to the code of practice. Obviously, that would set a higher test in the authority regimes than is currently envisaged under the Bill. I cannot table such an amendment now, but the Committee

> will want to know that I am considering those matters and that we intend to return to them on Report (Hansard, 2000c).

The issue was not returned to in the Commons, however, and a recommended amendment from Heald was dropped as a result of the promise of later consideration.

The issue was returned to in the Lords Committee Stage, after further pressure from industry. When Lord Bassam introduced the list of amendments, he stated,

> We recognise that this is a crucial issue, especially for industry. We have received a number of representations on the issue from the British Chambers of Commerce and the Institute of Directors. We have tried to allay their concerns by explaining just what the Bill actually states and what it seeks to achieve. We have also received helpful correspondence not least from the British Bankers' Association setting out its understanding of the way in which Part III of the Bill works. In the light of those representations, we have decided to recast these provisions. … In recognition of the views of industry, we made wide changes to Clause 47 in another place to add an extra test if keys are to be required. That was welcomed and Members of the Committee have proposed further changes. We have suggested our own amendments, which take account of the views of industry and cover the majority of points raised by the Committee. (Hansard, 2000e Column 962).

The 'extra test' was allowing for the release of any key, thus addressing the granularity issue.

In addition to the amendments allowing notification to the corporate directors, shortly thereafter some within industry, including the BCC (but not necessarily the authors of the commissioned report), eased their opposition to Part III of the Bill (Clarke, 2000a).

6.2. Burden of proof

The next issue of contention, of less direct interest to industry, but under much scrutiny, was the reverse burden of proof issue. It was first raised within Parliament by the Conservative Shadow Home Secretary in the House of Commons Second Reading:

> Clause 49 creates the offence of failing to comply with such a notice. Yet the nature of the offence is such that the burden of proving an innocent explanation for failure to provide the key is laid at the door of the accused; in other words, people are presumed guilty unless they can prove that they are innocent (Hansard, 2000b Column 781).

The Home Office minister responded to this accusation at the time on the basis of differing interpretation:

> (T)he burden falls on the prosecution to prove beyond reasonable doubt that the accused is, or has been, in possession of a key and that he or she failed to comply with the notice. The Bill outlines several statutory defences. …Innocent people will not suffer under the provisions. As I pointed out, we believe that the Bill is ECHR compatible. (Hansard, 2000b Column 834).

To expand the point against criticism, Clarke continues:

> Clause 49(2) creates a defence for an individual who has forgotten or mislaid a key or password. It is true that he or she must prove the defence, but they need to do that only on the balance of probabilities. In other words, he or she must explain what has happened. It will be for the court to decide whether, on balance, the person is telling the truth. That seems to be an entirely reasonable burden to impose on an accused person. (Hansard, 2000b Column 883).

The Home Office Minister then states that such a practice is not uncommon in other statutes.

These arguments were repeated at the Second Reading within the House of Lords when Lord Bassam, a Home Office Minister, stated in return to criticism to the section:

> (W)e took issue with the suggestion that the offence reverses the burden of proof. It has also been suggested that individuals can be locked up for two years for forgetting a password. We do not believe that that is likely. We have set out in detail in another place the reasons why we do not believe that it will happen. None the less, we welcome continued debate on how the construction of the offence might be improved (Hansard, 2000f Column 884).

Further debate ensued, and concern arose in the news media to an even higher level. However, the opinion and beliefs of the Home Office changed when the Home Office Minister introduced amendments to the Committee Stage in the House of Lords:

> We have tabled amendments that make it clear that proof of previous possession can lead to a conviction. However, it will not do so if the defendant raises an issue about whether he still has possession of the key. Once that happens, the burden falls back on the prosecution in the normal way (Hansard, 2000e, Column 1009).

This was met with approval from the Committee, as Lord Cope, the Conservative Lord responsible for much of the opposition to the Bill, stated "I am glad that the Government have moved on the question of burden of proof. It was important that they should do so" (Hansard, 2000e, Column 1012).

Amendments did not come to an end after the Home Office's proposed changes. There was a late amendment in Report stage, introduced by The Lord Cope and The Viscount Astor that inserted the requirement that the accused must knowingly fail to make the disclosure of plaintext or key. Lord Bassam approved of such an amendment:

> The changes made to the non-compliance offence in Committee have been broadly welcomed. (The amendment) will, I believe, offer some further comfort. The amendment means that Clause 51 would say that a person is only guilty of an offence if he knowingly fails to comply with a disclosure requirement imposed upon him. So some kind of inadvertent failure to comply would not be penalised. That was the point of the earlier debate and appears to be the issue behind the amendment of the noble Lord, Lord Cope. …(W)e are happy to make clear that unwitting failure should not be—and will not be—penalised (Hansard, 2000f, Column 442).

While the majority of the amendments were introduced by the Home Office, the previous

amendment, and the amendments given below were introduced by non-Home Office peers relating to the security of disclosed keys.

6.3. Late amendment: security of keys

Two amendments were added at the Report Stage involving the security of the keys. The first required that the keys, once lawfully collected, are stored in a secure manner. The second amendment deals with liability incurred when the key is misused, a concern of industry. According to Lord Bassam:

> My Lords, this amendment addresses a concern that has been put to us on a number of occasions by industry. The concern is that once keys are seized under this legislation and notwithstanding the strict safeguards set out in Clause 55, there remains a possibility that keys could be compromised once they have been seized. Industry is rightly concerned to ensure that that possibility is minimised and that proper sanctions exist in case it occurs. We agree that it would be wrong for the consequences of insecure safeguarding to fall on the owners or users of keys. We also agree, as I indicated on Report, that the duty imposed on public authorities to look after keys should be actionable. In other words, if keys are insecurely stored the responsible public authority can be sued (Hansard, 2000f, Column 1073).

Again, these changes were to alleviate the concerns of industry and the costs, risks, and liabilities associated with key disclosure (Whitley and Hosein, 2001).

6.4. Unchanged issues

The RIP Bill received a significant amount of criticism in the media, in Parliament, industry, and among civil liberties organisations (Wadham, 2000; Whitley and Hosein, 2001). The peak of the pressure was at the time of Lords Committee and Lords Report stages. At the Committee stage, many of the amendments from the opposition peers were made redundant, as a result of Home Office amendments. By the Lords Report stage, the opposition peers managed to introduce a selection of amendments, however many were rejected.

The most powerful and controversial amendment that was rejected lost by one vote: the amendment would have required Secretary of State authorisation on each occasion a key (rather than plaintext) was demanded, thus effectively checking the volume of access requests and creating some procedural oversight. The state of affairs remains that all such requests need only be authorised by senior members of the police.

Additional rejected amendments include the requirement that when an individual is given a plaintext decryption notice, the authorities must also present the encrypted text for decryption at the same time as the notice; and to avoid the situation of surrendering keys when the authorities do not trust the decryption process, a procedure was recommended where a trusted third party could demonstrate the link between the ciphertext and the plaintext.

A most interesting failed amendment would have dealt with government's dual-interests and concerns of jurisdictional arbitrage: if other countries failed to enact similar legislation, the proposed amendment would have rescinded Part III of the Bill and thus

would have alleviated the off-shore threat, and concerns about human rights. The amendment was rejected, however.

According to Caspar Bowden, director of the think-tank FIPR, as the Bill left the Lords, "It's Zombie legislation. Although clinically dead with macabre wounds, it still lumbers on menacing both individual privacy and commercial confidence" (FIPR, 2000).

7. Lessons from the RIP Bill

The goal of this paper has been to outline the challenges in establishing a policy habitat to support electronic commerce. By reviewing the specific case of the UK, from its first mentioning of the regulatory intents regarding encryption in 1996 through to the Royal Assent of the Regulation of Investigatory Powers Act in July 2000, some strategic issues can be determined.

There are many possible explanations for the introduction of the RIP Bill. One was the need to update the Interception of Communications Act, both as a result of technological advances and in order to comply with the new Human Rights Act. The felt need for government to support electronic commerce also contributed, as did the Home Office's concerns with the proliferation of encryption techniques that were necessary for electronic commerce, but also more available because of the Internet. The changing shape of the market place also had an impact as new businesses outside the scope of existing legislation, for example, Internet service providers, were becoming major players in the economy and in the provision of communications services.

Earlier interventions in the electronic commerce arena had taken various forms. An initial attempt at regulation of one element of electronic commerce was attempted, i.e. the mandatory licensing of Trusted Third Parties. This, however, was not successful and was replaced by a voluntary regime which was ineffective in practice. The DTI then introduced regulatory interventions in the form of the Electronic Commerce Bill, and sections were later divided between the Electronic Communications Act and the Regulation of Investigatory Powers Act.

After the draft electronic commerce bill was split in two, the Home Office took over the more contentious aspects that related to law enforcement issues. This was a result of a great deal of controversy over concerns that surveillance considerations were overriding legitimate regulatory needs within electronic commerce. The Home Office assumed responsibility for the surveillance aspects with its own update of the Interception of Communications Act 1985. However, unlike the DTI and the Cabinet Office, the Home Office's expertise is not in liasing with the business community and many of the problems the legislation faced could be seen to arise from this, as the industry opposition was intense (BCC, 2000; ISPA, 2000).

By studying the progress of the regulation from 1996, and particularly the trajectory of the Bill through Parliament, it is possible draw lessons from the experience of the British Government. In particular, it is possible to highlight five issues that similar legislation may have to address as other countries try to establish similar policies (as is currently occurring in Australia, France, New Zealand, South Africa, and is occurring in international conventions such as the Council of Europe (2001)).

First, there is the conflict between secure transactions and the need for certain bodies to be able to access them. Governments will wish to *update* (Hosein, 2001) their laws to deal with secure transactions enabled through encryption, but there are at least two clear interests at stake: encryption supports electronic commerce and shields criminal activity. UK acknowledged this from its very first articulation of encryption policy, but then spent many years realising that dealing with criminal activity through regulation affected electronic commerce as well. Even when the initiatives were split into two separate statutory instruments, the law enforcement instrument, the RIP Bill, still contained measures that affected electronic commerce.

Second, the articulated costs and risks of implementing any such lawful access capabilities will have an impact on the growth of Internet activity in the country. The first set of proposals from the British government involved an onerous regulatory regime of trusted third parties, and the costs and risks associated with operating such an institution were considered too high for the market to adopt, amongst other reasons. The earlier proposals also failed to differentiate between the types of keys, such as signature and encryption keys, and as a result introduced risks to electronic commerce (Abelson et al., 1998). Under access provisions in the RIP Bill, the risk of key disclosure and misuse were concerns of industry (as articulated in the BCC report (2000)). The settlement was the establishment of a liability minimisation regime, and notice sent to corporate directors in the case of keys belonging to employees that were accessed and specific keys.

Third, the practical implications of seizing encryption keys for ongoing surveillance leads to interesting technological and human rights implications. The technological issues were addressed with the granularity of the keys: after amendments, individuals can now select which keys are disclosed (subkeys, session keys, etc.). The human rights issues involve particularly due process considerations. This includes an authorisation process for accessing keys where a judge signs the warrant (as promised in the Labour Manifesto), or the Home Office Secretary signs the warrant (as in a failed amendment); the treatment of reverse burden-of-proof of lost/destroyed keys, which was addressed to some extent in an accepted amendment; and the issue surrounding self-incrimination, which has not yet been resolved. Other countries with differing respect for human rights and due process (the US is among the highest with this regard to due process, less developed countries often have the least regard) may interpret and develop policy around these issues differently but will at least have to consider them.

Fourth, governments must attempt to legislate within the context of a rapidly changing technological environment. Often times in the Hansard the parliamentarians noted that all these issues would have to be revisited as the technology continued to change. Moreover, bypassing the statutory powers of RIP is not technologically challenging, and as a result the Act may have to be revisited to increase its applicability; as this was addressed late in the parliamentary debates, the line of questioning was dismissed. The model of regulation selected by the British government is designed ideally for such revisiting, however: primary legislation, being the RIP Act, and associated Codes of Practice that are still being negotiated even over a year later.

Finally, the reality of a global infrastructure and the nature of commerce involving information and communication technologies implies that regulation that imposes too much on industry may result in a situation of regulatory arbitrage as companies or services

move off-shore. This was raised particularly by the BCC report how companies may choose to store their keys off-shore where they may not be compromised by the British law enforcement agencies; or more simply technical solutions can be found to place keys just beyond access. The most interesting articulation of this issue was the rejected amendment to remove the government access to keys provisions in a sunset clause if other countries failed to adopt similar legislation. On the last day of debate before Royal Assent, Mr. Clarke defended the bill and the global implications:

> After the Bill receives Royal Assent, we shall work with the industry—and the Opposition, if they are willing—to promote it both in this country and internationally. Given the comments made in the overseas media, we must explain clearly what the Bill is and is not, and why we do not believe it poses a threat to e-commerce in Britain; on the contrary, it will help to achieve the Government's aim of a strong and secure e-commerce economy, to which we are all committed.
> Propaganda is needed, and I hope that the whole House will help to promote the interests of this country's businesses when the time comes.

The point is being pursued in the Council of Europe draft convention on cybercrime (as critiqued in (Global Internet Liberty Campaign, 2000)), which contains ambiguous statements regarding lawful access (Council of Europe, 2001, article 19.4), and as other countries pursue similar regulatory regimes, the British may not be alone for much longer with these powers, and resulting in less countries for industry to which to relocate.

These strategic issues that arise in the creation and settlement of national policies on electronic commerce are not unique to the UK. Varying consultation processes in other countries may give rise to varying results and instruments, however it is our belief that many of the issues raised in this policy process will either be raised again in other countries, or other governments may learn from the pioneering experiences of the UK. Interpretive flexibility may result based on existing statutory environments (such as bills of rights and constitutions), applicability and decisions of criminality (what is considered a serious crime?), and the amount of consideration given to industry and electronic commerce interests (costs reimbursement and infrastructure considerations); but so long as there is consultation, debate, and discourse the strains and implications as seen in the UK may still apply.

The technological environment surrounding electronic commerce, as articulated above, necessarily includes encryption and the Internet itself. Both of these technologies, and the according environment played a rôle in the development of the British policy as the technological environment is one of the key components to the habitat of electronic commerce policy. The traditional policy habitat of commerce has been transformed by renewed interest in technologies such as the Internet and encryption that are enabled and driven by electronic commerce; as a result the policy habitat of electronic commerce is different to that of traditional commerce. New regulations are thus introduced to deal with these new problems. Whether it is discussion of authentication and digital signatures or a discourse surrounding the surveillance capacities of the state, it is our contention that the lessons discussed above may be raised in other national legislatures when the time comes. Regulating this political, legal, technological, and commercial habitat is a challenge worthy of further study; as the UK has learned.

Acknowledgements

The authors would like to thank Simon Davies and Caspar Bowden for their assistance in explaining the intricacies of the Bill and its implications; Robin Mansell and Andrew Murray for commenting on earlier drafts and the anonymous reviewer for useful comments. Professor Roger Needham was instrumental in obtaining funding from Microsoft Research UK which supported some of this work.

References

Abelson, H., Anderson, R., Bellovin, S.M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Neumann, P.G., Rivest, R.L., Schiller, J.I., Schneier, B., 1998. The risks of key recovery, key escrow, and trusted third party encryption. http://www.cdt.org/crypto/risks98.

Akdeniz, Y., 2001. Case Analysis of League Against Racism and Antisemitism (LICRA), French Union of Jewish Students, v Yahoo! Inc. (USA), Yahoo France, Tribunale de Grande Instance de Paris, Interim Court Order, 20 November 2000. Electronic Business Law Reports 1 (3), 110–120 Archived at www.cyber-rights.org/documents/yahoo_ya.pdf.

Angell, I.O., 2000. The New Barbarian Manifesto: How to Survive the Information Age. Kogan Page, London.

Armey, D., 2001. Letter to the House of Representatives: Privacy: For those who Live in Glass Houses. April 9, 2001.

Baldwin, R., Cave, M., 1999. Understanding Regulation: Theory, Strategy, and Practice. Oxford University Press, Oxford.

Baldwin, R., Abel-Smith, B., Cave, M., Fenn, P., Hodges, M., Marsden, C., Mossialos, E., Scott, C., Woolcock, S., 1995. Regulation in Question: The Growing Agenda. Merck Sharp and Dohme, London.

Baldwin, R., Scott, C., Hood, C., 1998. Introduction. In: Baldwin, R., Scott, C., Hood, C. (Eds.). A Reader on Regulation. Oxford University Press, Oxford.

BCC, 2000. The Economic Impact of the Regulation of Investigatory Powers Bill: An Independent Report Prepared for the British Chambers of Commerce. British Chambers of Commerce.

Beath, C.M., Orlikowski, W.J., 1994. The contradictory structure of systems development methodologies: deconstructing the IS-user relationship in Information Engineering. Information Systems Research 5 (4), 350–377.

Beatson, J., Eicke, T., 1999. In the Matter of the Draft Electronic Communications Bill and in the Matter of a Human Rights Audit for Justice and FIPR. Archived at http://www.fipr.org/ecomm99/commaud.html.

Beck, U., 2000. What is globalization?. Polity Press, Cambridge trans Camiller, P..

Braithwaite, J., Drahos, P., 2000. Global business regulation. Cambridge University Press, Cambridge.

Brown, I., Gladman, B., 2000. Technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses. Foundation for Information Policy Research Archived at http://www.fipr.org/rip/RIPcountermeasures.htm.

Clarke, C., 2000a. Letter to the editor. The Daily Telegraph, 28 June 2000.

Clarke, C., 2000b. Letter to the editor: Crime and the net. The Daily Telegraph, 13 July 2000.

Council of Europe, 2001. Draft Convention on Cybercrime, version 27 with Convention and Explanatory Memorandum Archived at http://conventions.coe.int/treaty/EN/projets/cybercrime27.doc.

DTI, 1996. Paper on Regulatory Intent Concerning use of Encryption on Public Networks. Department of Trade and Industry Archived at http://www.fipr.org/polarch/regint.html.

DTI, 1997. Licensing of Trusted Third Parties for the Provision of Encryption Services Public Consultation Paper on Detailed Proposals for Legislation. Department of Trade and Industry Archived at http://www.fipr.org/polarch/ttp.html.

DTI, 1998. Secure electronic commerce statement. Department of Trade and Industry Archived at http://www.fipr.org/polarch/secst.html.

DTI, 1999a. Building Confidence in Electronic Commerce. Department of Trade and Industry Archived at http://www.dti.gov.uk/cii/elec/elec_com_1.html.

DTI, 1999b. A report for the DTI summarising responses to Building Confidence in Electronic Commerce. Department of Trade and Industry URN 99/89 Archived at http://www.dti.gov.uk/cii/elec/conrep.htm.

ECB, 1999. Electronic Commerce Bill. Archived at http://www.fipr.org/polarch/draftbill99/partIII.html.

European Union, 1995. Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L281.

European Union, 1997. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. Official Journal L024.

European Union, 2000. Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector. Document 500PC0385.

FIPR, 1999. Analysis of the (draft) electronic communications act 1999. Foundation for Information Policy Research Archived at http://www.fipr.org/uk_ecomm_bill/index.html.

FIPR, 2000. News release: second and final day of the house of lords report stage debate on the regulation of investigatory powers bill. Foundation for Information Policy Research Archived at http://www.fipr.org/rip/PRLordsReport.txt, 13/7/2000.

G8, 1997. Meeting of justice and interior ministers. Archived at http://www.g8summit.gov.uk/prebham/washington.1297.shtml.

Global Internet Liberty Campaign, 2000. Member Letter on Council of Europe Convention on Cyber-Crime Version 24.2. Archived at http://www.gilc.org/privacy/coe-letter-1200.html.

Goldsmith, J., 2000. Unilateral regulation of the Internet: a modest defence. European Journal of International Law 11 (1), 135–148.

Hague Conference on Private International Law, 1999. Preliminary Draft Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters. Archived at http://www.hcch.net/e/conventions/draft36e.html.

Hahn, R.W., 2001. The Costs of Online Privacy Legislation Revisited. AEI-Brookings Joint Center.

Hansard, 2000. House of Commons 9th February 2000 (First Reading).

Hansard, 2000b. House of Commons 6th March; 2000 (Second Reading).

Hansard, 2000c. House of Commons Committee 4th April 2000 (Committee Stage).

Hansard, 2000d. House of Lords 25th May 2000 (Second Reading).

Hansard, 2000e. House of Lords 28th June 2000 (Committee Stage).

Hansard, 2000f. House of Lords 13th July 2000 (Report Stage).

Heinz, J., 1991. US Strategic Trade: An Export Control System for the 1990s. Westview Press, Colorado.

Home Office, 1999. Interception of Communications in the United Kingdom: A Consultation Paper. Home Office Archived at http://www.homeoffice.gov.uk/oicd/interint.htm.

Home Office, 2000. Myths and Misunderstandings. Home Office Archived at http://www.homeoffice.gov.uk/ripa/myths.htm.

Hood, C., 1994. Explaining Economic Policy Reversals. Open University Press, Buckingham, England.

Hosein, I., 1998. Consultation and contemplation: what has gone before: a summary of the first UK cryptography policy consultation process. , 1998 Electronic Privacy Information Center Sourcebook. EPIC, Washington DC.

Hosein, I.G., 2001. The collision of regulatory convergence and divergence: updating policies of surveillance and information technology. To be published in The Southern African Journal of Information and Communication.

ISPA, 2000. Response to the Smith Group Report for the Home Office on Technical and Cost Issues Associated with Interception of the Internet. Archived at http://www.fip.org/rip/lSPA_response_Smith_19.6.2000.htm.

Klein, H.K., Myers, M., 1999. A set of principles for conducting and evaluating interpretive field studies in information systems. MIS Quarterly 23 (1), 67–93.

Labour_Party, 1997. Manifesto.

Latour, B., 1992. Where are the missing masses? The sociology of a few mundane artifacts. In: Bijker, W.E., Law, J. (Eds.). Shaping Technology/Building Society: Studies in Sociotechnical Change. The MIT Press, Cambridge, MA, pp. 225–258.

Latour, B., 1999. Pandora's Hope: Essays on the Reality of Science Studies. Harvard University Press, Cambridge, MA.

Law, J., Hassard, J., 1998. Actor Network and After. Blackwell, Oxford 0-631-21194-2 0-631-21194-2.

OFGEM, 2000. OFGEM: bringing choice and value to gas and electricity customers. Archived at http://www.ofgem.gov.uk/.

OFSTED, 2000. Welcome to the Office for Standards in Education (OFSTED), officially the Office of Her Majesty's Chief Inspector of Schools in England. Archived at http://www.ofsted.gov.uk/.

OFWAT, 2000. Welcome to the Office of Water Services (OFWAT). The economic regulator for the water industry in England and Wales Archived at http://www.ofwat.gov.uk/index.htm.

Peltzman, S., 1989. The Economic Theory of Regulation after a Decade of Deregulation. Brookings Papers on Microeconomics.

PIU, 1999. Encryption and Law Enforcement, a Cabinet Office Report. Performance and Innovation Unit Archived at http://www.fipr.org/polarch/piu.pdf.

Postman, N., 1992. Technopoly: The Surrender of Culture to Technology. Vintage Books, New York.

Pouloudi, A., Whitley, E.A., 2000. Representing human and non-human stakeholders: on speaking with authority. In: Baskerville, R., Stage, J., Gross, J.I.D. (Eds.). Organizational and Social Perspectives on Information Technology. Kluwer, Aalborg, Denmark, pp. 339–354.

Roszak, T., 1994. The Cult of Information: A Neo-luddite Treatise on High-Tech, Artificial Intelligence, and the True Art of Thinking. University of California Press, Berkeley.

Seguin, E., 2000. The UK BSE crisis: strengths and weaknesses of existing conceptual approaches. Science and Public Policy 27 (4), 293–301.

Shenk, D., 1997. Data Smog: Surviving the Information Glut. Abacus, London.

Straw, J., 2000. Letter to the editor: bill will not cause e-commerce to decamp. Financial Times, 15th June 2000.

Swarbrick, D. 1999. David Swarbrick analyses the potential human rights infringements from the Electronic Communications Bill 1999. Law Gazette, 1999(6). Archived at http://www.lawgazette.co.uk.

Wadham, 2000. Letter to the editor of the daily telegraph: dangerous bill. Daily Telegraph, July 12, 2000.

Wallace, J., Mangan, M., 1997. Sex, Laws and Cyberspace. Owl Books, New York.

Walsham, G., 1993. Interpreting Information Systems in Organisations. Wiley, Chichester.

Whitley, E.A., Hosein, I., 2001. Doing politics around electronic commerce: opposing the regulation of investigatory powers bill. In: Russo, N., Fitzgerald, B., DeGross, J.I. (Eds.). IFIP Working Group 8.2 Conference on Realigning Research and Practice in IS Development: The Social and Organisational Perspective. Kluwer, Boise, Idaho, pp. 415–438.

Yahoo Inc Vs La Ligue Contre Le Racisme et L'Antisemitisme, 2001. C-00-21275 JF. United States District Court for Northern California: San Jose Division Fogel J.