28 DOING POLITICS AROUND ELECTRONIC COMMERCE: OPPOSING THE REGULATION OF INVESTIGATORY POWERS BILL

Edgar A. Whitley
Ian Hosein
London School of Economics and Political Science
Houghton Street
London WC2A 2AE
United Kingdom

Abstract

Providing an environment for electronic commerce involves complex, technical questions that need to be addressed and understood by decision making bodies. This paper studies one attempt to support electronic commerce at the national level. It looks at the Regulation of Investigatory Powers Bill in the UK and focuses on the political actions of those seeking to amend the Bill in Parliament. After presenting the situation, the paper analyzes the actions in terms of a due process model of political action. The paper presents the results of this analysis and reflects on the implications for theory and practice.

1. INTRODUCTION

From the first moment that information systems were conceptualized in terms of the interaction between computing technology and human activity systems (Checkland 1981), questions of politics have been a part of the discourse around the implementation and use of systems. The political element of information systems has most commonly been seen in terms of organizational questions surrounding the implementation of new computer systems (Markus

1983). Others have viewed systems development in terms of wider political questions, for example in terms of labor relations and employee empowerment (Kyng and Mathiassen 1982; Mumford 1983), gender relations (Everts 1998) and autonomy and control (Winner 1977).

Political issues must also be considered at more macro levels, as organizations and systems extend beyond national jurisdictions. The globalizing potential of information and communication technologies is highlighted as a contributing factor to the capacity of transnational organizations to no longer be constrained by national boundaries (Angell 2000), or emphasizing practical limitations for national governments to control content (Wallace and Mangan 1997), data flows, and crime. The intersections between political action and new technologies are also seen when governments attempt to implement national information infrastructure projects (National Research Council 1994; West 1996), or when technology is considered to support existing statutory powers and norms (IETF 2000) or when technology is designed with aspects that circumvent traditional state powers (Anderson 1997).

Political action is also associated with information technology when governments seek to create legislative frameworks that support or encourage new trends such as electronic commerce, or address issues such as the "digital divide" (U.S. Department of Commerce 2000). While the tools available to information systems researchers are becoming increasingly sophisticated for understanding organizational politics, they are far less refined for understanding political action at the national level (Silverstone and Mansell 1996).

This paper adds to this understanding of the politics surrounding information and communication technologies at the national level by considering the opposition to a recent piece of legislation in the United Kingdom, the Regulation of Investigatory Powers Act (RIP 2000). This detailed piece of legislation was widely opposed and was heavily amended during its progress through the parliamentary process. As such, it provides a rich resource from which detailed understanding of the political process can be gained. Moreover, the debate about the proposed Act, both in the media and in parliament, is available in publicly accessible documents, which form the basis for the analysis.

Section 2 introduces the need to provide a secure environment for electronic commerce and shows how the RIP Bill sought to support this. The paper then introduces a model of due process, which is used to analyze the political process involved in opposing the Bill. This addresses the two main forms of opposition to the Bill: the report sponsored by business and the activities of a think tank. Some outcomes of the political debate are described. The paper then analyzes the political processes associated with the act in terms of the model of due process and the implications for our understanding of the political process and the due process model are described. The paper ends with a summary of the paper and a discussion of the implications raised.

2. SECURE ELECTRONIC COMMERCE AND THE REGULATION OF INVESTIGATORY POWERS ACT

Electronic commerce has grown significantly in recent years and has now reached a stage where it has the potential to become a significant part of most developed economies. As such, national governments have begun to become concerned with the role that they should be playing to ensure that e-commerce could fulfill this potential for their economies, although many governments began thinking about this before e-commerce had taken off. Despite the techno-libertarian views of many involved in the new media, governments have traditionally been involved in most economic activities, providing a relatively peaceful, mostly prosperous, environment that makes wealth creation possible (Borsook 2000).

Unfortunately, it is not immediately apparent what governments should do to support electronic commerce because the requirements for successful electronic commerce may conflict with other requirements traditionally seen as within the scope of government activity (taxation, consumer protection, etc.). One of the greatest such conflicts arises with secure electronic commerce. That is, for electronic transactions such as Internet transactions to be acceptable, some certainty and reliability needs to be established between trading partners. The details of the business transaction need to be shared, and when some of this data is valuable, the sharing must be done confidentially (as in credit card numbers, bank account numbers, etc.). The integrity of the shared data needs to be verified, to ensure that a business transaction requesting one book has not been changed to a request for 10 books. In a converse example, some form of protection against a client fraudulently claiming to have ordered only one book when the order was originally for 10 means that some form of non-repudiation is also required. To some extent, the business transaction also requires authentication; that is, consumers need to know that they are dealing with bookstore.com and not booksore.com, which may be fraudulently seeking to mimic the legitimate store. Cryptography is generally accepted as a part of the solution to provide the required security for Internet transactions: confidentiality, integrity, authentication, and non-repudiation.

If electronic commerce uses encryption technology to secure its business transactions, this same technology can potentially be used by those involved in criminal activities for transactions over the Internet and this forms the basis of the government's dilemma. In order to support electronic commerce, it should encourage the strongest forms of encryption that are technically feasible (Blaze et al. 1996). Indeed, the normally apolitical Internet Engineering Task Force has called for the strongest form of encryption available (IETF 1996). Unfortunately, these same techniques can be used for criminal activity, to the

disadvantage of law enforcement agencies (White House 1996) that will find themselves unable to access Internet transactions concerning criminal activity. If government ensures that law enforcement agencies are able to have access to all encrypted Internet transactions, then confidence in the security of electronic commerce will be limited.

This was the dilemma facing the UK government, which, despite having a clear strategy to help make the UK "the best place in the world for e-commerce" (Office of the e-Envoy 2000), introduced the RIP Bill to Parliament stating that the Bill was 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 [sic], tobacco smuggling and other serious offences (Hansard 2000a Column 768).

Initially, the UK government sought to address both potential and controversial applications of cryptography, that is for electronic commerce and for criminal use, into a single piece of legislation (DTI 1997). However, for practical reasons, it ended up splitting the legislation into two different acts.

The first, the Electronic Communications Bill, became law in 2000. The second, the Regulation of Investigatory Powers Bill, which was to contain the law enforcement provisions with respect to investigations involving the use of encryption, was then introduced. While encryption was the focus of part III of the Bill, the opportunity was taken to revitalize law enforcement powers dealing with communications generally, and thus to update the Interception of Communications Act 1985. The RIP Bill was of concern because of its possible impact on encryption and interception on electronic commerce. There were additional concerns that, because of the interception components within the RIP Bill (and its extension to the Internet), this would create burdens on Internet Service Providers (ISPs) and thus raise the costs and risks of doing electronic commerce in the UK, resulting in some ISPs choosing to move services offshore. Another concern was that it would introduce potential points of failure into the network and, more generally, weaken the competitiveness of the UK economy. The Regulation of Investigatory Powers Bill was introduced to Parliament on February 9, 2000, and was passed on July 28, 2000.

This Bill, which has been dubbed "the snoopers charter," was the focus of concerted, political protest and as a result was changed significantly during debates in Parliament. Patricia Hewitt, the E-Minister with overall responsibility for e-commerce policy, has admitted that not "everything was right in the first version of the RIP Bill" (Mathieson 2000), which runs counter to the claims

made when the Bill was first introduced that it was well thought out, having been the result of detailed engagement with "serious commentators" (Clarke 2000). Hewitt believes that the Bill was greatly improved as a result of "very extensive parliamentary debate" (Mathieson 2000) and while it is true that the RIP Bill was one of the most heavily amended Bills in recent parliamentary history, this statement does not explain why the Bill was so heavily amended, nor does it indicate which issues were considered as necessary for amendment.

This then, forms the basis of the situation to be analyzed. The government introduced a piece of legislation seen by many to be problematic. There was considerable organized opposition to the Bill. Two agents were particularly active in opposing the Bill. First there was a report commissioned by the British Chambers of Commerce (BCC) and second there was the continuous work of the Foundation for Information Policy Research (FIPR). Others involved in the lobbying/briefing process included Charles Lindsey, a former academic, who advised some of the Lords, and other organizations such as LINX (London Internet Exchange), the Institute of Directors, the Internet Service Providers Association (ISPA), and the Confederation of British Industry. Their involvement was more limited, however, so this paper will focus on two key actors: the BCC report and FIPR. Both play key roles in the political process although, as the Bill is amended during the normal parliamentary process, their involvement is by definition indirect. The situation is further complicated by the fact that, although many involved in coordinating the opposition to the Bill had experience addressing other pieces of technology related legislation, very little has been written about the political process they undertook. In particular, it appears that they did not follow any predetermined strategy for organizing their activities. One of the purposes of this paper, therefore, is to try and understand the political action and learn lessons from it in terms of our understanding of regulation, representation, and the politics of technology (Introna and Nissenbaum 2000).

The analysis of this piece of political action begins with the presumption that the effects of the political action are at a distance (Rose and Miller 1992) and that communication (through briefings and reports) plays a key role in the process (Cooren 2000). This perspective suggests that many of the concepts associated with actor network theory (Law and Hassard 1998) could be used to understand the political process. A model of political process that uses these concepts is introduced in the next sections; the paper then considers the report commissioned by the British Chambers of Commerce (BCC 2000) and the lobbying activities of FIPR before analyzing them in terms of the due process model.

3. POLITICAL ACTION FOR TECHNOLOGICAL ISSUES

There are many ways of studying how the changes to the Bill came about, including theories of regulation and institutional economics. This paper, however, will use ideas developed from actor network theory. In particular, it draws upon questions of representation of entities (both human and non-human), the role of experts in dealing with technical issues, and the work involved in building and maintaining collectives.

In particular, this paper maps the political process of opposing the RIP Bill in terms of a model for the politics of nature proposed by Bruno Latour (1999). This model has three stages: (1) introducing possible entities for consideration in the political sphere, (2) discussing whether they actually contribute to the issue under discussion, and then (3) developing a political settlement which incorporates a selection of the candidate entities (Latour 1999).

At first sight, such a mapping might seem counter-intuitive as the authors of the BCC report were not following any particular political strategy, and by implication not Latour's model, when writing their report. Similarly, FIPR were not explicitly seeking to introduce new candidate entities or maintain the existence of other entities for consideration by parliament. However, useful insights can be drawn by looking at the previously described process from this perspective. Moreover, the analysis can also contribute back to Latour's model by demonstrating the complexities of actual political processes.

Latour's model starts with the suggestion that governments often face problems when dealing with technical questions. As Dewey (1946 p. 136) states

> the questions involved, questions of science, agriculture, industry and finance, are highly technical. How many voters are competent to measure all the factors involved in arriving at a decision? And if they were competent after studying it, how many have the time to devote to it? It is true that this matter does not come before the electorate directly, but the technical difficulty of the problem is reflected in the confused paralysis of the legislators whose business it is to deal with it.

This problem is magnified still further when dealing with situations where the infrastructure is still forming, as is the case with Internet security. While it is tempting to trust the experts, the additional challenge of encompassing all possible forms of technology that might exist meant legislators had to deal with a "moving target" every step of the way.

First, there is the inability to capture all technical issues around the interception of Internet transactions. In part, this arises because the legislation was proposed by the Home Office rather than, say, the Department of Trade and Industry. Although some external experts were used by the Home Office, their involvement was limited to the earlier stages of the process (Smith Group 2000). Another reason for this situation was the government's attempt to be "technology neutral" in its policy:

> Charles Clarke: I make it clear to hon. Members and to people outside the House that we shall not force anyone to use a particular technology. Individuals and businesses remain free to utilise any type of encryption, provided they choose the one that best suits their needs (Hansard 2000a, Column 834).

The debate also was concerned with the "forming" of the infrastructure for electronic commerce and e-business. In the House of Lords, this was raised with respect to encryption and Internet transactions:

> Lord Lucas: What really frightens people about the way in which the clauses are drafted is that because they will be pretty useless against the serious criminal they will be used only against casual traffic, and, more important, will be available for use against messages received and communicated by substantial international businesses. Anyone who uses the Internet, which is essentially an open system—there is nothing secure about it—must use a high level of cryptography and assure clients, customers and associates that his systems are secure. Anything that puts that in doubt or makes business believe that by conducting this activity in the UK it lays itself open to international law suits or merely produces a loss of confidence that data stored in the UK is not as secure as data stored in a country which is not governed by this kind of legislation, even with the latest government amendments, will result in a substantial loss of business to this country (Hansard 2000d, Column 934).

Similarly, there is a third area of concern: framing the legislation only around (our understanding of) today's technology. In the second reading of the Bill, the Secretary of State states:

> Mr. Straw: Our goal is to make the United Kingdom the best and safest place in the world to do e-commerce. The industry,

> too, wants a secure environment in which to conduct business. The scheme of the Bill is aimed at trying to keep up with the advance of technology as best we can (Hansard 2000a, Column 777).

While attempting to maintain powers in a new environment, however, there is concern over the rate of change of technology.

> Mr. Gapes: The Home Secretary said that we needed to keep up with the advance of technology as best we can. The Bill is necessary and probably overdue. However, I suspect that, in a few years time, it will be out of date. I hope that it will not be left for too long on the statute book—that has happened to other measures—before we review it and update it if necessary (Hansard 2000a, Column 786).

Latour proposes a model for dealing with complex questions in situations such as these for which there is no clear answer, drawing on insights from science and technology studies. The model has a particular concern for due process and the avoidance of political shortcuts by those with particular technical expertise (Latour 1997).

4. AVOIDING SHORT CUTS: A MODEL OF DUE PROCESS

Many technical or scientific questions do not have definitive answers; rather, they are still often in a state of considerable flux. It is only over time that particular answers become accepted as facts. Thus, while there is growing consensus about the causes of global warming, the explanations do not have the same status as, for example, those about gravity. During scientific and technical controversies, technical experts cannot be relied upon to provide the definitive answer (Collins and Pinch 1998).

Instead, what they can do is suggest things that they believe should be taken into consideration when devising policy and it is likely that different experts will make different suggestions of things to consider. For example, many scientists argue that chlorofluorocarbons (CFCs) are a major cause of global warming and hence that the use of CFCs in refrigeration processes should be eliminated over time (EPA 2000b). In a similar way, environmental groups argue that the exhaust emissions from cars also contribute to global warming and some believe that all cars should be banned (Car Free Cities 1998) while others believe that

tax systems should be modified to discourage car usage and encourage more environmentally friendly transportation (EPA 2000a).

This intuition has been developed into a model of a political process by Latour (1999). The first stage (which consists of presenting candidate "entities" for consideration) he labels with the question "how many are we?" and involves the proposal of candidate entities and discussion of which should be taken into consideration at that time (for example, CFCs and car exhaust emissions are seen as suitable entities for inclusion in political debate about global warming). The second stage, labeled with the question "how can we live together?," involves taking the entities accepted in the first stage and proposing action based on them. In the global warming case, this means government legislation to outlaw the use of CFCs, combined with progressive taxes to discourage the use of cars rather than the more extreme step of banning all cars.

When developed into a model for politics, this approach avoids the risk of short-cutting (whereby technical experts "decide" what is the best course of action based on their own understanding) and ensures that a due process is followed (McMaster et al. 1999). Moreover, the model is inherently temporal. Those candidate entities that are not taken into consideration at any one point in time can always "appeal" the decision and be considered in future iterations (Whitley 1999).

Thus having described the due process model, it is now possible to use it in conjunction with a description of the actual political processes associated with the Bill. This paper examines two sets of activities: the report by the British Chambers of Commerce and the lobbying activities of FIPR in terms of the introduction, consideration, and possible adoption of various entities both human and non-human.

5. OPPOSITION TO THE BILL: THE BCC REPORT

The UK business community, in conjunction with privacy advocates, undertook a major lobbying 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 issues covered by the Bill that hadn't been understood properly or taken into account fully. In particular, the British Chambers of Commerce commissioned a report into the economic impact of the proposed Act. The commission came about in part as a response to consultations with privacy advocates about the RIP Bill.

With hindsight, it is apparent that this report played a major role in the debate. In particular, it ceased to simply be a statement by the business community about its concerns regarding a particular piece of legislation. Instead, it

can be seen as a means by which a number of "overlooked" issues were represented and introduced into the public debate (Pouloudi and Whitley 2000). Again, with hindsight, the decision to publish the report with the BCC byline, rather than a Privacy International byline as initially intended by some of its authors, meant that their "industry" voice could be used to say things that wouldn't be listened to normally.

The BCC report does this through a process of "thick description." By describing, in considerable detail, the implications of the proposed legislation, it introduces a large number of new entities into the political discussion.

A striking example of this can be found in section A of the report. Here the authors seek to understand how the process of intercepting Internet data will be implemented, emphasizing how different it is from interception under the plain old telephone system (POTS). For example, if the interception aim is to intercept e-mail messages, then this can be done by taking advantage of the store-and-forward nature of e-mail systems. In the case of a simple mail transfer, all that is required is to make a copy of any mail messages going to or from the target's e-mail account through servers. However, if this is to be done effectively for law enforcement purposes the issue immediately becomes more complex.

> Of course, making a copy of the email is only the start of the process. The email needs to have various forensic information added (time stamps, identity of target, place of interception and so forth). It then needs to be securely sent to the Government's GTAC [Government Technical Assistance Centre] for passing onward to the correct agency who wanted the interception done (BCC 2000, Section A.1).

Moreover, "information on the targets for interception is classified information at the SECRET level and hence requires special handling using appropriate government security procedures" (BCC 2000, Section A.1).

Interestingly, the BCC report understated the added complexity of intercepting e-mail messages going to web-based accounts such as hotmail, yahoo mail, etc. In these cases the messages are not going out with mail headers from the user's access point to the Internet (presumably a network access point at the ISP); rather, they are http headers and thus law enforcement agencies need to be able to intercept all tcp/ip based user traffic in order to find the e-mail. This situation also seems to arise with the U.S. Carnivore system (Dooley and Plesser 2000).

Thus, by describing in detail what needs to be done to implement the Act, the BCC report is undertaking political action by giving a voice to the "missing

masses" (Latour 1992), both human and non-human, that the drafters of the Bill had overlooked (in particular, the issues that had not been raised by the government sponsored Smith report [Smith Group 2000], which formed part of the background to the debate about the legislation and in particular focused on practical implementation issues). Some of the missing entities identified by the BCC report are listed in the box, drawing on the thick description of the process given in Appendix 1.

In addition to highlighting the existence of these entities, the BCC report also seeks to represent them in terms of the costs they will contribute to the implementation of the Act. In total, they contribute at least £13,000,000 in costs per annum and are part of the headline figure of £46 billion over five years which the report claimed the Bill would cost the UK economy. (The remainder of this sum is made up of losses and leakage from the UK economy resulting from the reductions in electronic commerce activity, the relocation of servers outside the UK and the opportunity costs of network managers of UK ISPs spending time and money dealing with interception rather than working on improving the network efficiency (Clayton 2000)).

The figure of £46 billion was widely reported in the press when the report was first issued (Davies 2000; Eaglesham 2000; Hirst 2000; Tringham 2000; Wintour 2000) and so the BCC report can be seen to be making these extra entities part of the public discourse about the Bill (even if they are only indirectly part of the figure of £46 billion being discussed).

Candidate Entities	**Likely Cost (per Annum)**
ISP staff authorized to access SECRET data	£500,000
Interception equipment suitable for handling SECRET data	£10,500,000—£16,000,000
Secure accommodation for interception equipment	£1,000,000
Secure network connecting the ISPs and GTAC in central London	£1,000,000–£10,000,000
At present, the Home Office does not have standards for equipment that can connect systems containing SECRET information to the Internet. These must be developed.	Unknown
Total	**£13,000,000—£27,500,000**

The Home Office, who were responsible for the Bill, repeatedly denied that the costs would be as high as £46 billion over five years. In a letter to the editor of *The Financial Times*, Jack Straw, the home secretary, stated:

> It will also be reassuring to your readers to learn that having headlined as fact the ridiculous claim that the Bill will cost the economy "£46bn," you now say this figure was "never more than illustrative." That is true—but it is illustrative only for a fevered imagination and some very poor arithmetic (Straw 2000)

before restating the claim that the UK is creating a "competitive advantage for the UK for electronic commerce, and one—with this bill—in which industry as well as our citizens are better protected from serious criminal attack" (Straw 2000).

The letter was handed by Mr. Straw to *Financial Times* journalist at a press conference, "after accusing the newspaper of giving too much credence to the report prepared by the London School of Economics for the British Chambers of Commerce" (Burns et al. 2000) although it was also claimed that the size of the e-commerce market project in Mr. Straw's letter appeared to contradict the Department of Trade and Industry's own forecasts. The Home Office set up a "Myths and Misunderstandings" website about the BCC report which dealt, amongst other issues, with the figure of £46 billion. According to the Home Office, "The figure has no foundation. It is clear that the BCC clearly do not believe this themselves. They have not asked for the Bill to be scrapped" (Home Office 2000a). These myths and misunderstandings pages are still being listed by the Home Office on its web page about the Act (Home Office 2000b) and have been updated due to errors and misunderstandings of their own.

If the BCC report was seen as introducing new entities into the debate, then the statements by the Home Office can be seen as attempts to remove these entities from the debate. Unfortunately, in this case, it would appear that removing entities is far more difficult than introducing them, and despite the best efforts of the Home Office, the figure of £46 billion (and hence the entities that make it up) is still being quoted (Hall 2000; Rohde 2000; Sheriff 2000).

The different estimates of costs were discussed in Parliament and, while some speakers accepted the Home Office's position and suggested that the legislation would introduce no new costs, others thought the figures quoted by the BCC report were more realistic. For example, Lord Cope, speaking in the House of Lords stated:

> my original understanding was that the sum of £20 million was the estimated cost of the black boxes, part of which was to be borne by the Government and part of which was to be borne by the ISPs.
>
> However, my subsequent understanding was that the sum of £20 million was the total cost of the Government's contribution to the scheme. That implies that the total cost of the black boxes will be higher than that.…Whatever sum of money is paid by service providers—however large or small—will damage the competitiveness of British service providers compared with those overseas who do not have this overhead (Hansard 2000c, Columns 1024/1025).

6. OPPOSITION TO THE BILL: FIPR BRIEFINGS

If the BCC commissioned report became the focal point for initial media interest in the opposition to the Bill, during the parliamentary passage of the Bill, particularly during the committee stages of the House of Lords, the Foundation for Information Policy Research undertook the role of coordinating the briefings of MPs and members of the House of Lords.

The authors of the BCC report have close links with FIPR (Nicholas Bohm, Ian Brown, Richard Clayton, Simon Davies, Brian Gladman, and Gus Hosein are all members of the Advisory Council to FIPR) and were often involved in assisting FIPR and its director, Caspar Bowden, in its briefings. FIPR's website also acted as a central repository for archived copies and links to all media reports about the Bill. As a matter of policy, FIPR aims to include links to *all* relevant information about the Bill that it is made aware of. As the Bill progressed through parliament (see the box), the FIPR site recorded the debates and the proposed and actual amendments to the Bill.

FIPR's briefings were not always seen positively. For example, Baroness Thornton expressed concern about the methods that have been employed by the Foundation for Information Policy Research, pointing out that it was funded, in part, by Microsoft (Hansard 2000b, Column 412).

Others, however, spoke in favor of the briefings. For example, Lord Phillips of Sudbury, responded, arguing that

> if the noble Baroness, Lady Thornton, believes that we are under the control of the foundation to which she referred, she gives little credit to the many noble Lords on this side of the House. That foundation is an extremely public-spirited one. The fact that it receives money from Microsoft does not align

House of Commons
RIP Bill Introduction, February 9, 2000
Second Reading, March 6, 2000
Committee Stage, March 28—April 4, 2000
Third Reading, May 8, 2000

House of Lords
Introduction, May 9, 2000
Second Reading, May 25, 2000
Committee Stage, June 12—June 28, 2000
Report Stage, July 12, 2000
Third Reading, Two Sittings, July 19—July 20, 2000

House of Commons
Commons Consideration of Lords Amendments, July 26, 2000
Royal Assent, July 28, 2000

(Adapted from http://www.homeoffice.gov.uk/ripa/ripleg.htm)

> it with the devil. Without its assistance many of us on these and other Benches would have been a good deal more befuddled than we already are (Hansard 2000b, Column 414).

Indeed, during the third reading, the role of FIPR was formally acknowledged by Lord McNally (Hansard 2000c, Column 1081)

In addition to briefing members of Parliament and the House of Lords, FIPR also introduced some new entities into the debate themselves. A FIPR paper (Brown and Gladman 2000), written by two authors of the BCC report, on technological means of circumventing the RIP Bill, was introduced on the last day of debate before the Bill received the Royal Assent. The paper showed that the envisaged powers for interception and for the seizure of encryption keys were technically obsolete. That is, the paper outlined how individuals could take steps to preserve their privacy regardless of the powers presented by RIP through various methods, including selecting a small ISP (which was unlikely to be required by government to have interception capabilities installed); moving the e-mail server off-shore (and thus outside of the jurisdiction of UK law enforcement agencies); or making use of advanced technology (IPv6) to encrypt packets individually. It was briefly mentioned on the final day of consideration of the Bill in the House of Commons, but was effectively ignored.

Through its briefings and clarifications, FIPR helped ensure that the new entities introduced into the debate by the BCC report were not discarded simply on the basis of not understanding the often complex issues raised by the implementation of the Act and also tried to introduce new entities into the debate at the last moment.

7. POLITICAL SETTLEMENT

The final version of the Bill that became law in July 2000 was vastly different from the one introduced to Parliament six months earlier. This paper has described a number of issues that the BCC report raised. These issues continued to play a role in the parliamentary debate, in part as a result of FIPR's clarifications and briefings. Many of these were incorporated into amendments for the final version of the Bill.

Inevitably a compromise figure about the extra costs associated with implementing secure interception of secret data was reached and the government agreed to share a higher proportion of the costs incurred by ISPs. In so doing, implicit acknowledgment was made of the need to consider these extra entities in the political process, even if the costs associated with them were disputed. Additionally, a technical advisory board was formed which would oversee the implementation of intercept capabilities, with a particular brief to monitor technical feasability issues and costs.

As stated earlier, the technical entities involved in circumventing the Bill (Brown and Gladman 2000) as it stands were ignored. Although these entities were ignored by Parliament, presumably criminals can still communicate without concern of interception by the law enforcement authorities. This may give rise to a situation where the Home Office may, in the future, request that the Act be revisited to consider the issues raised within the FIPR paper.

8. APPLYING THE MODEL

In this section, the activities of the BCC report and FIPR are considered in relationship to the various stages of the due process model outlined above.

Time T_1, Step 1: At this stage, the BCC report seeks to introduce a number of candidate entities into the political discussion. These are business related issues and they are represented in terms of costs. At the same time, the Department of Trade and Industry is also seeking to affect the entities that will be considered and attempts to discount the extra entities raised by the BCC report. FIPR seeks to clarify questions about the candidate entities to ensure that they are not eliminated at this stage due to misunderstandings.

Time T_1, Step 2: The parliamentary process does, in fact, take into consideration the entities raised by the BCC and the broader costs of implementing the Act are discussed in Parliament.

Time T_1, Step 3: As a result of the parliamentary process, Parliament arrives at a piece of legislation with which it is comfortable and this is given the Royal Assent on July 28, 2000.

The political process does not stop at this point but rather begins consideration of the next time frame (**Time T_2, Step 1**) by marshaling new candidate entities. Of particular importance for the RIP Act is the implementation of the European Convention on Human Rights, which became law on October 2, 2000. Although the government believes that the RIP Act is compatible with the Human Rights Act, there are plans to challenge it in the courts. Thus the abstract notion of human rights (or, more particularly, its concrete implementation as the Human Rights Act) is a candidate entity for consideration when the Act is revised. Politically, the two main opposition parties in the UK have issued statements that they intend to look at the Act again if they come to power. Furthermore, as discussed above, changes in technology may also make it necessary to revisit the Act.

9. COMPLICATIONS

The experiences of the FIPR briefing on circumvention illustrate one limitation of Latour's model when applied to the practical experiences of forming legislation. The due process of Parliament took six months for this Bill. In response to issues raised by parliamentarians, FIPR introduced a further set of entities at the very end of the parliamentary process, namely the means by which the Act could be circumvented. If the Latourian model is mapped temporally onto the parliamentary process, this FIPR intervention occurs in Time T_1, Step 3, although in practice the action is logically associated with Time T_1, Step 1. Similarly, although these technical issues were debated at the Time T_1, Step 3, in practice their status is similar to that of entities excluded from the parliamentary debate as a whole at Time T_1, Step 1. As such they are eligible for reconsideration later. The next iteration of the process (Time T_2, Step 1) will, therefore, need to consider questions relating to the technological advances raised by the FIPR report, in addition to more general technological developments.

Another complication relates to the ways in which proxy representatives were used for the new entities considered in the BCC report. Rather than discussing the effects of the proposed Act on ISP managers, ISP office space, ISP systems, etc., they are all compounded into a single "cost" figure. While it can be argued that this is one of the roles of money (Callon 1998), it is not an ideal solution to the question of political representation.

10. SUMMARY AND FURTHER QUESTIONS

This paper has reviewed the political process associated with opposing a piece of legislation that was intended to enable the development of electronic commerce in the United Kingdom. In particular, the paper sought to analyze this process in terms of the raising of new entities that ought to be considered in the political debate, deciding on which entities to take into consideration for action, and then implementing political action.

As such, it maps nicely onto a model of political action developed by Latour. Further useful insights into the political process and the limitations of Latour's model can be drawn from this mapping.

Although the paper deals with political action at the national level, a very similar process can be seen to occur in the political debate surrounding the introduction of new information systems, where different stakeholders (Pouloudi and Whitley 1997) or actors (Checkland 1981) will all seek to introduce entities into the discussion of the new system. Most implementation processes involve some form of consultation with interested parties and the processes outlined in this paper provide one way of improving them.

The paper and political process described within it raises further legitimate questions which cannot be addressed in detail here. In particular, there are important questions about how the opponents of the Bill attained a media voice at all, as well as questions about how they ensured that all viewpoints were considered. It is hoped that these will be dealt with in a further paper that will show the link between media interventions and changes to the Bill more explicitly.

More generally, it is possible to apply the model back on the political process undertaken by FIPR and the authors of the BCC report themselves. By giving voice to overlooked entities, a proper political process should ensure that in so doing it is not causing other entities to be overlooked. Thus, by having the BCC report explicitly focus on the business costs of the proposed Act (and including as many such costs as it could to come up with its headline figure of £46 billion), it was explicitly not raising issues associated with civil liberties, human trafficking, etc. While there may be some practical reasons for doing so, they do not enable a truly fair and open process that considers all possible aspects of the debate, and there is a risk that the BCC report is doing its own shortcutting of due process by focusing on business costs and thus ignoring these other issues in the same way as the government's technical experts.

Other concerns with the process as implemented in practice can be raised with the government's consultation stages. As the paper has shown, the claim was that the Bill was the result of widespread consultation with industry, yet this feeling was not shared by many industry insiders. For example, the Internet Service Providers Association, in its response to the initial Smith Report, stated:

> The Government has talked a lot about its consultations with industry—which comes as somewhat some surprise to ISPA. In several months of discussions we have hardly clocked up a full six hours of talks with the Home Office and so we're still at the stage of explaining the problems and have hardly started to look for practical solutions (ISPA 2000)

11. ACKNOWLEDGMENTS

The authors gratefully acknowledge conversations with Simon Davies and the other authors of the BCC report and members of FIPR. François Cooren's comments on the paper were also very helpful. Particular thanks to Bruno Latour for suggesting the notion of politics by "thick description" and Ole Hanseth for giving a longer slot than expected at the Tromsø meeting, which led to this paper. An earlier version was presented to Media@LSE and benefitted from the helpful comments of participants, including Roger Silverstone and Sonia Livingstone.

12. REFERENCES

Anderson, J. R. "The Eternity Service," *Pragocrypt'96*, 1997 (archived at http://www.cl.cam.ac.uk/users/rja14/eternity/eternity.html).

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

BCC. *The Economic Impact of the Regulation of Investigatory Powers Bill: An Independent Report Prepared for the British Chambers of Commerce*, London: British Chambers of Commerce, 2000 (archived at http://is.lse.ac.uk/Research/BCC RIPA.pdf).

Blaze, M., Diffie, W., Rivest, R., Schneier, B., Shimomura, T., Thompson, E., and Wiener, M. *Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security: A Report by an Ad Hoc Group of Cryptographers and Computer Scientists,* 1996 (rchived at http://www.counterpane.com/keylength.html).

Borsook, P. *Cyberselfish: A Ccritical Romp Through the Terribly Libertarian World of High-Tech*, London: Little, Brown and Company, 2000.

Brown, I., and Gladman, B. *Technically Inept: Ineffective Against Criminals While Undermining the Privacy, Safety and Security of Honest Citizens and Businesses*, Foundation for Information Policy Research, 2000 (archived at http://www.fipr.org/rip/RIPcounter measures.htm).

Burns, J., Eaglesham, J., and Shrimsley, R. "NATIONAL NEWS: Straw Attacks Critics of e-mail Intercept Bill," *Financial Times*, June 15, 2000, p. 6.

Callon, M. (ed.). *The Laws of the Markets*, Oxford: Blackwell, 1998.

Car Free Cities. *About Car Free Cities*, 1998 (archived at http://www.edc.eu.int/cfc/).

Checkland, P. *Systems Thinking, Systems Practice*, Chichester, England: Wiley, 1981.

Clarke, C. "Letter to the Editor: Crime and the Net.," *The Daily Telegraph*, July 13, 2000.

Clayton, R. *Speech at Scrambling for Safety 2000*, 2000 (archived at http://www.fipr.org/sfs2000/).

Collins, H., and Pinch, T. *The Golem: What You Sshould Know About Science* (2nd Edition), Cambridge: Canto, 1998.

Cooren, F. *The Organizing Property of Communication*, Amsterdam: John Benjamins, 2000.

Davies, S. "How Your Privacy Could Soon RIP: Simon Davies Fears Government Plans for Online Surveillance Will Devastate E-commerce," *The Daily Telegraph*, July 12, 2000.

Dewey, J. *The Public and Its Problems: An Essay in Political Inquiry,* Chicago: Gateway Books, 1946.

Dooley, B. A., and Plesser, R. L. *The Legal Standard for Government Tracing of Internet Communications: The Misuse of Pen Register Court Orders for Real-Time Acquisition of Transactional Information*, Commercial Internet Exchange Association, 2000 (archived at http://www.cix.org/WhitePaper.pdf).

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

Eaglesham, J. "WORLD NEWS: UK: 'E-snooping' Measure Pits Government Against Apprehensive Business Leaders," *Financial Times*, June 23, 2000, p. 11.

EPA. *Global Warming: Actions, Transportation*, Environmental Protection Agency, 2000a (archived at http://www.epa.gov/globalwarming/actions/transport/index.html).

EPA. *Global Warming: Emissions*, Environmental Protection Agency, 2000b (archived at http://www.epa.gov/globalwarming/emissions/index.html).

Everts, S. *Gender and Technology: Empowering Women, Engendering Development*, London: Zed Books, 1998.

Hall, S. "Email Spy Laws Costly and Undemocratic," *Guardian Unlimited*, September 20, 2000 (archived at http://www.guardianunlimited.co.uk/Archive/Article/0,4273,4065743,00.htm).

Hansard. "House of Commons 6th March, 2000 (Second Reading)," 2000a.

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

Hansard. "House of Lords 19th July, 2000 (Third Reading)," 2000c.

Hansard. "House of Lords 28tj June, 2000 (Committee Stage)," 2000d.

Hirst, C. "Business: Blair Pledge on e-mail Snooping," *Independent on Sunday*, July 2, 2000.

Home Office. *Myths and Misunderstandings*, Home Office, 2000a (archived at http://www.homeoffice.gov.uk/ripa/myths.htm).

Home Office. *Regulation of Investigatory Powers Page*, Home Office, 2000b, (archived at http://www.homeoffice.gov.uk/ripa/ripact.htm).

IETF. *RFC 1984: Statement on Cryptographic Technology and the Internet: Status: Informational*, Internet Architecture Board and Internet Engineering Task Force, 1996, (archived at http://www.ietf.org/rfc/rfc1984.txt?number=1984).

IETF. *RFC 2804 Policy on Wiretapping: Status: Informational*, Internet Architecture Board and Internet Engineering Task Force, 2000, (archived at http://www.ietf.org/rfc/rfc2804.txt?number=2804).

Introna, L. D., and Nissenbaum, H. "Shaping the Web: Why the Politics of Search Engines Matters," *Information Society* (16:3), 2000, pp. 169-185.

ISPA. *Response to the Smith Group Report for the Home Office on Technical and Cost Issues Associated with Interception of the Internet*, Internet Service Providers Association, 2000 (archived at http://www.fipr.org/rip/ISPA_response_Smith_19.6.2000.htm).

Kyng, M., and Mathiassen, L. "Systems Development and Trade Union Activities," in *Information Society: For Richer for Poorer*, N. Bjørn-Andersen, M. Earl, O. Holst, and E, Mumford (eds.), Amsterdam: North Holland, 1982.

Latour, B. *Politiques de la nature. Comment faire entrer les sciences en démocratie*, Paris: La Découverte, 1999.

Latour, B. "Socrates' and Callicles' Settlement—or, the Invention of the Impossible Body Politic," *Configurations* (5:2), 1997, pp. 189-240.

Latour, B. "Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts," in *Shaping Technology/Building Society: Studies in Sociotechnical Change*, W. E. Bijker and J. Law (eds.), Cambridge, MA: The MIT Press, 1992, pp. 225-258.

Law, J., and Hassard, J. (eds.). *Actor Network and After*, Oxford: Blackwell, 1998.

Markus, M. L. "Power, Politics and MIS Implementation," *Communications of the ACM* (26:6), 1983, pp. 430-444.

Mathieson, S. "A Year in the Life of an E-minister," VNU Business Publications Limited, September 22, 2000 (archived at http://www.vnunet.com/Features/1111447).

McMaster, T., Vidgen, R. T., and Wastell, D. G. "Networks of Association and Due Process in IS Development," in *Information Systems: Current Issues and Future Changes*, T. J. Larsen, L. Levine, and J. I. DeGross (eds.), Laxenburg, Austria: IFIP Press, 1999.

Mumford, E. *Designing Secretaries: The Participative Design of a Word Processing System*, Manchester: Manchester Business School, 1983.

National Research Council. *Realizing the Information Future: The Internet and Beyond*, National Academy of Sciences, 1994 (archived at http://www.nap.edu/readingroom/books/rtif/.

Office of the e-Envoy. *e-Commerce*, 2000 (archived at http://www.e-envoy.gov.uk/2000/strategy/strategy.htm).

Pouloudi, A., and Whitley, E. A. "Stakeholder Identification in Inter-organizational Systems: Gaining Insights for Drug Use Management Systems," *European Journal of Information Systems* (6:1), 1997, pp. 1-14.

Pouloudi, A., and Whitley, E. A. "Representing Human and Non-human Stakeholders: On Speaking with Authority," in *Organizational and Social Perspectives on Information Technology*, R. Baskerville, J. Stage, and J. I. DeGross (eds.), Boston: Kluwer Academic Publishers, 2000.

RIP. *The Regulation of Investigatory Powers Act*, Her Majesty's Stationary Office, 2000 (archived at http://www.hmso.gov.uk/acts/acts2000/20000023.htm).

Rhode, L. "UK e-mail Law Reaches U,S.," *Infoworld*, September 4, 2000, pp. 28-29.

Rose, N., and Miller, P. "Political Power Beyond the State: Problematics of Government," *British Journal of Sociology* (43:2), 1992, pp. 173-205.

Sheriff, L. "Lib Dems Go Against RIP Bill," *The Register*, September 20, 2000 (archived at http://www.theregister.co.uk/content/6/13405.html).

Silverstone, R., and Mansell, R. "The Politics of Information and Communication Technologies," in *Communication by Design: The Politics of Information and Communication Technologies*, R. Mansell and R. Silverstone (eds.), Oxford: Oxford University Press, 1996., pp. 213-228.

Smith Group. *Technical and Cost Issues Associated with Interception of Communications at Certain Communication Service Providers*, The Smith Group Limited, 2000 (archived at http://www.homeoffice.gov.uk/ripa/techcost.pdf).

Straw, J. "Letter to the Editor: RIP Bill is Tightly Drafted to Protect Us All," *Financial Times*, June 19, 2000.

Tringham, M. "Fury Over Law on e-mail, Premier Executive," *The Times*, June 22, 2000.

U.S. Department of Commerce. *Falling Through the Net: Toward Digital Inclusion— A Report on Americans' Access to Technology Tools*, U.S. Department of Commerce, Economic and Statistics Administration, and National Telecommunications and Information Administration, 2000 (archived at http://www.ecommerce.gov/PressRelease/fttn00.pdf).

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

West, J. "Utopianism and National Competitiveness in Technology Rhetoric: The Case of Japan's Information Infrastructure," *The Information Society* (12:3), 1996, pp. 251-272.

White House. *Statement of the Vice President*, The White House, Office of the Vice President, 1996.

Whitley, E. A. "Habermas and the Non-humans: Towards a Critical Theory for the New Collective," in *Proceedings of the Critical Management Studies Conference*, C. H. J. Gilson, I. Grugulis, and H. Willmott (eds.), Manchester School of Management, July 14-16, 1999. (archived at http://www.mngt.waikato.ac.nz/ejrot/cmsconference/documents/Information%20Tech/Habermas%20and%20the%20non-humans.pdf).

Winner, L. *Autonomous Technology: Technics-Out-of-Control as a Theme in Political Thought*," Cambridge, MA: The MIT Press, 1977.

Wintour, P. "Policy and Politics: Internet Spy Bill Set at Pounds 20m.," *The Guardian*, July 7, 2000, p. 15.

About the Authors

Edgar Whitley is a senior lecturer in Information Systems at the London School of Economics and Political Science. He has a B.Sc. (Econ) Computing and a Ph.D. in Information Systems, both from the LSE. He has taught undergraduates, postgraduate students, and managers in the UK and abroad. Edgar was one of the organizers of the First European Conference on Information Systems and is actively involved in the coordination of future ECIS conferences. He has published widely on various information systems issues and is currently editing a special issue of *The Information Society* on Time and Information Technology. He is one of the program chairs for the forthcoming IFIP 8.2 conference on organizational discourse and information technology to be held in Barcelona in December 2002. Edgar can be reached by e-mail at E.A.Whitley@lse.ac.uk.

Ian (Gus) Hosein is a doctoral student in Information Systems at the London School of Economics and Political Science. Since 1997, he has lectured to undergraduate and postgraduate students on topics including networks and computer security, the concept of the Information Society, and the political and regulatory interests in technology. He has also presented at institutions including Cambridge University, Johns Hopkins, and the University of Witwatersrand. His area of research is technology policy, with a core concentration on national and international initiatives, focusing on secure communication techniques. Through his work with Privacy International, the Foundation for Information Policy Research, and Zero-Knowledge Systems, he has also spoken at OECD, UNESCO, and Royal Institute for International Affairs sponsored events, and participated at G8 and Data Protection Commissioners conferences. He is a survivor of a B.Math Hons. Applied Mathematics (University of Waterloo), and a M.Sc. ADMIS (LSE). More information is available at http://is.lse.ac.uk/staff/hosein. Gus can be reached by e-mail at I.Hosein@lse.ac.uk.

APPENDIX 1

SOME OF THE CANDIDATE ENTITIES LISTED BY THE BCC REPORT

ISP Staff

ISP staff are required to assist in the process of identifying and routing target traffic to interception points and this will mean that system administrators will have access to government data classified as secret and will all have to be appropriately cleared.

For small ISPs, only a small number of staff will be involved, but it would be impossible to reduce this number below two. For large ISPs, many staff are likely to be involved in system administration although it might be possible to clear only a subset of them. Using a figure of 10 staff for each large ISP and two for each small one suggests that 300 staff in total could have knowledge of interception targets. Assuming that staff change every three years, 100 new staff each year would have to be cleared and trained in the handling of Government classified material. Using an estimate of £2,000 per clearance, £1,000 for staff training and costing 10% of staff salaries against such duties, the resulting overall costs would be of the order of £500,000 per annum.

ISP Located Interception Equipment Costs

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

ISP Accommodation Costs

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

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

The accommodation costs involved in some large ISP locations will be very high. In locations such as Telehouse in London, the enormous growth in both the number of ISPs and the physical size of their network and computer systems is already placing a huge strain on the available space with the result that any equipment space is at a high premium. If government interception requirements add to the volume of equipment involved, ISPs are certain to face severe difficulties in locations such as this where space is not available. It may, hence, be necessary for an ISP to reconfigure its existing systems to accommodate this additional equipment. The costs involved in building and housing equipment capable of handling secret information is difficult to estimate without a precise knowledge of the character and physical location of all the ISPs involved. However, a reasonable estimate of these costs would be £5,000 per annum for a small ISP and £50,000 per annum for a large ISP. Using the earlier ISP numbers, this results in costs of £1,000,000 per annum.

GTAC Interface Costs

The technology to safely connect systems containing secret information to the Internet does not exist and this is recognized in government regulations for

handling secret data, which do not allow such connections. Given this situation, it is far from obvious how interception systems that contain secret information about the targets of interception could ever be connected to the Internet, but this appears to be what the Home Office intends to do. Since it is not currently feasible to meet this requirement, it must be assumed that the Home Office intends to carry the risks involved in such connections. The Smith report does include network firewalls at a number of critical points in the interface between ISP and the GTAC delivery network, but it seems most unlikely that the cost and risk issues of handling secret information on the GTAC side of such interfaces have been fully assessed. The additional costs involved have not been estimated here because there is no sound basis on which to do this given that the required technology is not available.

GTAC Secure Network Costs

The Home Office cost estimates do not appear to include the costs of the secure network required to connect between ISP locations and the GTAC site in central London. The costs of such a network would be very high if it were to be dedicated to GTAC use, but it seems more likely that an existing or planned government secure network will be used to meet this need. This will greatly reduce interception costs since this program will only have to bear a small part of the total cost. But it is not quite this simple. For GTAC to use existing or planned government secure networks will require that these networks include all ISP locations, a new requirement that will have significant cost and security implications for the network or networks in question. If GTAC traffic and other government traffic flows on a common network that includes many non-government nodes at ISP sites, the vulnerability and risk assessment for the network will change radically. Such consideration will increase the cost of the network for other users and these additional costs would need to be attributed to the interception requirement. Even in a shared network situation, the costs are likely to be very significant.

An idea of the costs involved in wide area secure networks can be gained by looking at MOD experience where costs are several hundreds of millions of pounds for implementation and several tens of millions of pounds for annual operating costs. However these networks support very high bandwidths and, more importantly, are designed to survive a full scale attack on the UK. The cost figures would be a great deal higher than those for a secure network to support GTAC. Operating a national network capable of handling secret data will not be cheap and the interception requirements will need to bear their share of such costs. These costs seem most likely to be in the one to ten million pounds per annum range based on the ISP numbers used earlier.