Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Telecommunications Policy 29 (2005) 857–874
TELECOMMUNICATIONS POLICY
www.elsevierbusinessandmanagement.com/locate/telpol

Policy discourse and data retention: The technology politics of surveillance in the United Kingdom

Edgar A. Whitley*, Ian Hosein

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

Abstract

This article presents an analysis of UK legislation on the retention of communications data that was introduced in the aftermath of the attacks of September 11, 2001. It presents a review of the discourses surrounding this legislation in parliament, in the wider international policy arena, in business and in terms of technology. The review of these discourses demonstrates that, in understanding policies involving a significant technological component such as communications data retention, policy alternatives may be evaluated only with an appreciation of technological characteristics alongside the traditional concerns of legislators, civil society and the business community. While academia has developed many forms of analysis for political, international, and regulatory discourses, the same must be undertaken for *technological discourse*, i.e. the interactions between the policies in question, the actors, and the technologies. Developing forms of analysis for technological discourses will likely lead to further understanding of both the policy problem and the actors' interests. The paper also shows how current institutions are slowly developing the necessary skills to incorporate the technological aspects of policy into political debate, and calls for a similar development for the law.
© 2005 Elsevier Ltd. All rights reserved.

Keywords: Data retention; Technology; Surveillance; Policy

1. Introduction[1]

The attacks on the US on September 11, 2001 have had far reaching impacts on all aspects of life, both in the US and throughout the world. Subsequent terrorist attacks in Bali, Istanbul, Madrid and London have also prompted responses from governments. One particular response has been the introduction of new legislation that seeks to address terrorist threats in terms of prevention, investigation and prosecution. In the US, these generally fall within the heading of "Homeland Security" and, in particular the USA-PATRIOT

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

[1]The authors have benefited from invaluable feedback from Gordon Gow and Robin Mansell. Earlier versions of this paper were presented to students taking Reima Suomi's telecommunications policy course at the University of Turku, Finland and the seminar organised by Paul Beynon-Davies at the European Business Management School, University of Wales Swansea, both of which provided useful feedback. The authors are also grateful for the support of Peter Shields and the comments of the anonymous reviewers who helped considerably in clarifying the argument of the paper.

0308-5961/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.telpol.2005.06.012

Act. Some of the technological challenges this and subsequent legislation raise have already been studied (Kerr, 2003; Yen, 2004).

The policy consequences of the attacks are not limited to the US; however, as many other governments and supranational bodies have also introduced new legislation in response to the attacks (EPIC, 2004). In the UK, the Anti-Terrorism Crime and Security Act 2001 introduced a broad range of powers, including the retention of communications data (the focus of this article). This is the practice of keeping all data that is related to communications transactions for an extended period of time in case this information is of value to government authorities.

The legislative changes on the retention of communications data were introduced rapidly and proved to be particularly controversial, both politically and economically. This article argues that to understand these policies reliance cannot be placed on the traditional models of policy analysis such as those based on economic and regulatory processes which were never designed to study such rapidly introduced policies. This is, in part, because the reduced timescales involved in proposing and implementing the legislation means that economic effects have not stabilised. This is also because of concerns about the particularities of the technological elements affected by the legislation (Hosein, Tsiavos, & Whitley, 2003). Meaning that technology plays a significant role both as a regulatory subject under the influence of political and economic forces and also as a regulator in itself, influencing the interests of traditional actors, and even changing the effects of traditional policies (Hosein et al., 2003). For example, Microsoft's Cryptographic Application Program Interface (CAPI) still implements and enforces restrictions on cryptographic service providers (CSPs) which requires them to be digitally signed (i.e., approved) by the US government, even after the original export controls themselves have been revised and made less restrictive (Hosein et al., 2003). The research presented in this paper is based on the assumption that alternative research strategies are more beneficial for studying such turbulent socio-technological environments, where the particularities of situations are significant (Suchman, 1987) and where it is important to obtain an immediate "impression" of the situation (Mlcakova & Whitley, 2004). In such cases, it would appear that language might show more stability than the marketplace. This paper therefore uses an analysis based on hermeneutic interpretation, language and discourse analysis to understand the policy on the retention of communications data (Introna, 1997; Yanow, 1996).

2. Discourse and the policy process

Understanding policy development is already complex. Adding technology adds even more complexity and raises fundamental questions about the relationship between technology, policy and politics (Latour, 2004).

One of the striking features of many areas of telecommunications policy is the speed by which its focus shifts as the technology changes. As technologies like mobile voice over IP emerge and digital convergence continues apace, policy in the area adapts and develops (e.g., Wu, 2004). Thus, technologies can be seen to have a direct impact on policies. But technology's effect is greater than that. Technological advances bring about changes to the whole nature of the debate, not just its content. Themes, policies and practices that had been particularly significant now appear passé. The debate about television standards is now likely to be expressed in terms of liberalisation rather than protectionism and particular technological characteristics of various domestic standards (c.f. Crane, 1978); the internet has replaced videotext, prestel and teletext as the key electronic publishing media and so has changed understanding of the very notion of publishing (c.f. Tyler, 1979). In other cases, the language that is used in discussions changes fundamentally. For example, the technological infrastructure that is the internet has dramatically changed the way notions of universal access are now discussed (Wynn, Whitley, Myers, & DeGross, 2003b).

The changes in language cause changes in the frames of reference that are used to discuss and ground the debate about the technology (Yanow, 1996). As a result it becomes ever more important to articulate the assumptions embedded in the language used to discuss telecommunications policies. In particular, these interpretations, articulations of constraints and voicing of concerns are points in policy discourses where "the technological" emerges from what is normally considered a "social" process of negotiation (Hosein, 2002). After all, if politics resides in the realm of the possible, what is considered possible is transformed by the technological, and possibly just as much as by the social. In discussion of content regulations, the nature of the infrastructure matters because much of the language of content regulations was devised for the centralised

national television broadcasting infrastructure rather than the distributed protocols of the internet. Similarly, "wiretapping" rules were devised with telegraph and telephone communications in mind, shaped by the technology as much as the rules were shaped by the centralised market structure. "Wiretapping" now exists within an environment that may lack wires, with more complex switching and market structure, and multiple borders, and other technologies including encryption and VoIP. Studying these policies today requires attention to these changing details, whether they arise in deliberation or not. The technological may emerge naturally, for example, by parliamentarians raising the details of protocols and algorithms in their debates and deliberations alongside more "traditional" issues of costs and benefits (Hosein & Whitley, 2002); it may be represented to meet political purposes, e.g., technology is described and defined in ways that furthers one's own interests (Pouloudi & Whitley, 2000) or it may be conceded for political purposes, e.g., ignoring technological details to knowingly enhance one's authority (Escudero-Pascual & Hosein, 2004).

In attempting to clarify the complex and yet conceptually improvised world view of the policy arena language shapes what can or cannot legitimately be talked about, researched, addressed, or solved; the language used sets up conventions and boundaries (Wynn, Whitley, & Myers, 2003a). Within the social sciences, the language that is used and the role it plays is understood within the broad notion of "discourse": discourse surrounding information technology, discourse surrounding social change or, in the case of this article, discourse surrounding a particular telecommunications policy, namely the question of the retention of communications data.

A key feature of the way discourse evolves, with or without consideration of the technological, is that it constrains and enables discussions, investment decisions and implementations, regardless of the particular merits of the language being used or the thread of the logic being followed. Every time this happens, decision makers draw on implied models of their organisation and its values, their technologies and of human behaviour in general. For example, in the case of the discourse about telecommunications policy and the retention of communications data, these assumptions encompass societal values like human rights, law enforcement issues and counter-terrorism as well as technological, business and commercial matters.

It is important to distinguish between the discourse surrounding the actual terminology commonly used to describe the problem being addressed and the deliberative process by which decisions are reached and influence exercised. Tracing the reasoning process, collecting the lines of argument, and observing the language used to describe sensitive issues allows us to make visible the terms, tokens, solutions, relationships and compromises that form the outcome of the deliberation (Yanow, 1996). In so doing it creates the context for future conversations. There may be incentives, therefore, to try and shape the language used in a particular debate by using (and not using) particular forms of discourse.

Most academic study of policy tends to focus on the implications of implementing a particular policy rather than its formation (Stigler, 1983, p. 541).[2] Nevertheless, the study of the policy formation process assists in understanding governance generally. Understanding the ever-changing mosaic of the "tapestry of varying forces and processes" (Baumgartner, Jones, & Wilkerson, 2002) that are "dynamic, fluid and closely joined" (Kingdon, 1995, p. 230) requires focusing on the negotiation and transformation of policy and institutions (Hood, 1994), the "public forums" that Rein and Schön (1993, p. 157) argue may "serve as institutional vehicles for policy debate".

The policy discourse therefore may include all stakeholders (Pouloudi & Whitley, 1997). Examination of this discourse involves analysis of the "interaction of individuals, interest groups and social movements and institutions, through which problematic situations are converted into policy problems, agendas are set, decisions are made, and actions are taken" (Rein & Schön, 1993, p. 145). In this article particular attention is paid to ways in which the discourse incorporates the technological (Majone, 1989, p. 70). By explicitly studying the wider picture of the policy discourse in this area, actors emerge from what Throgmorton (1991) calls different interpretive communities (e.g., scientists, politicians and lay advocates) who may be forced to engage in abnormal discourse as they debate across communities of practice (Boland & Tenkasi, 1995).

This paper therefore seeks to explore the discourses surrounding a particular piece of telecommunications policy, namely recent UK proposals on the voluntary retention of communications data for anti-terrorism, crime and security policies. It does this by proposing and exploring four main arenas where the debate about

[2]Exceptions exist that specifically focus on media policy (see, for example, Dutton, 1992; Mosco, 1988; Streeter, 1990).

this policy has evolved: in parliament amongst parliamentarians, ministers, and bureaucrats, the broader geopolitical context, the business environment and the specifics of the technology. In each case, the paper presents evidence of the discourses that surround the telecommunications policy in the area, both in terms of the specific language about the technology and the language of the debate and the ways in which the various actors attempt to structure each discourse. Showing how actors present particular representations of the technology to further enhance their own arguments, principles, and interests will aid understanding of politics (Latour, 2000).

The paper extends this process beyond just looking at the technology. Typically each discourse is the topic of a given paper. Thus studies could be conducted of the parliamentary discourse using the political sciences; the business context using regulation studies; the geopolitical context from the perspective of international law and relations; and the technological aspects from the sciences. Instead, this paper investigates each to show first that these all exist simultaneously, but secondly, to show that a deeper understanding of the policy emerges. It concludes by applying these discourses to the legal understanding of data retention to show how an appreciation of all the discourses further enhances its ability to comprehend policy and politics.

The structure of the paper is as follows. The next section introduces the basic concepts underlying the retention of communications data and outlines the time line for the various debates (both in parliament and elsewhere) in the UK context. Next the paper presents examples from the discourse in each of the four policy arenas outlined above. Finally, it draws together the various insights that the discourses in these different arenas bring towards an understanding of the policy process and, in particular, discourses that revolve around the particularities of technological artefacts (Akrich, 1992; Orlikowski & Iacono, 2001).

3. Definitions and time line

This section briefly explains what is meant by the retention of communications data in the context of the UK proposals. The intention is to introduce the key elements of this issue in as neutral way as possible, leaving the complications to emerge later in the debate.[3] At its simplest, *communications data* refers to the data "about" communications, rather than the data "in" communications (Kerr, 2003, p. 641). For example, Fig. 1, provides some sample communications data in the form taken from traditional, plain old telephone systems. The data consists of a number of elements, including, in this example, the date (first column), duration (second column), number dialed from (third column), number dialed to (fourth column) plus various items associated with technical service and routing data.

Note that nothing here refers to the content of the communication, it simply records what number called what number, when and for how long.

A policy on the *retention* of communications data involves storing all of this data, for all communications and transactions, for a period of time (and in particular, for longer than it would be kept for purely billing and engineering purposes). The *preservation* of data, in contrast, involves keeping the particular data about particular individuals' communications for a period of time (i.e., not routinely disposing of it), typically while suitable search warrants and subpoenas are generated.

Retention of data is of particular relevance to law enforcement agencies as these records may be the only physical traces left to show association between individuals or to put them in particular places at particular times (Home Office, 2003b, Section 5.5).

The particular policy that is being discussed in this article is the "Code of Practice for Voluntary Retention of Communications Data (under the Anti-Terrorism Crime and Security Act 2001)" (Home Office, 2003c) (henceforth "the Code") and as such is a direct result of the Anti-Terrorism Crime and Security Act 2001 (henceforth "ATCS") (HMSO, 2001a).

Shortly after the attacks on the US on September 11, 2001, the UK government introduced a bill to parliament seeking to amend the Terrorism Act 2000 (HMSO, 2000b) by introducing new powers to: "make further provision about terrorism and security; to provide for the freezing of assets; to make provision about immigration and asylum; to amend or extend the criminal law and powers for preventing crime and enforcing

[3]Reflexively, we note that in practice, even this description plays a role in shaping the discussion in this paper (see Woolgar, 2002, pp. 9–11).

```
19991003070824178165     0187611205      46732112106     -001----003sth   46      4673000---0013   14 10260
1999100307083041 33      01541011341     46708314801     -001----003sth   46      4670000-8 0013   11 10260
1999100307162963 51      0187614815      46739112106     -001----003sth   46      4673000---0013   13 10260
1999100307182788 74      015410124301    46708314801     -001----003sth   46      4670000-8 0014   11 10260
1999100307204736 18      0187614805      46739112106     -001----003sth   46      4673000---0013   14 10260
```

Fig. 1. Sample traffic data on the Plain Old Telephone System.

Labour Government Representatives
Mr David Blunkett, Home Secretary
Lord Rooker, Minister of State at the Home Office

Parliament - House of Commons
Mr Douglass Hogg (Conservative (Opposition Party))
Mr Jeremy Corbyn (Labour (Government Party))

Parliament - House of Lords
Lord McNally (Liberal Democrat)
Earl of Northesk (Conservative)
Lord Phillips of Sudbury (Liberal Democrat)

Fig. 2. Cited speakers from the parliamentary debates and roles at the time.

that law; to make provision about the control of pathogens and toxins; to provide for the retention of communications data; to provide for implementation of Title VI of the Treaty on European Union; and for connected purposes'' (HMSO, 2001a).

Part 11 of ATCS (HMSO, 2001b, Sections 102–107) concerns the retention of communications data. It states ''The Secretary of State shall issue … a Code of Practice relating to the retention by communications providers of communications data obtained by or held by them'' (Section 102.1). In the first instance, this Code will be voluntary (Section 102.4). ATCS laid out the process for issuing the Code which involved issuing a draft Code of Practice (Section 103.1.a) and consulting on it (Section 103.1.b) and placing the draft Code before parliament (Section 103.4). ATCS also allows the Secretary of State to make the Code of Practice compulsory (Section 104). ATCS did not include any provision for how to access the retained data, as this had been covered in the previous Regulation of Investigatory Powers Act (Akdeniz, Taylor, & Walker, 2001; HMSO, 2000a; Hosein & Whitley, 2002).

ATCS therefore did not directly introduce the process of data retention in the UK. Rather it set in place the mechanisms for issuing a consultation on a proposed Code that would be voted on, after consultation, some time later. ATCS was given the Royal Assent on December 14, 2001.

As with other anti-terrorism laws introduced in the immediate aftermath of terrorist attacks, a number of sunset provisions were included within ATCS. In particular, if the government failed to introduce a Code of Practice within 2 years (i.e., by December 13, 2003) the provision would lapse. Despite some contending that this would be the most effective way of quietly dropping a controversial piece of legislation, the Code was introduced and later approved on December 4, 2003.

4. Arena 1: parliamentary discourse about the code

It is apparent from this time line that one of the major debates about the Code took place in the UK Parliament. In particular, the UK process requires deliberation in the House of Commons, the House of Lords and finally in the House of Commons again, where discussion takes place of any amendments introduced by the House of Lords. In this section, relevant extracts from the parliamentary debate are presented, with Fig. 2 giving details of the affiliation of the spokespersons.

The Home Office, the ministry responsible for justice and internal affairs, sponsored the Bill. As a result, Home Office ministers introduced the Bill in the House of Commons and the House of Lords. The Labour Party has comprised the majority in parliament since 1997, and as a result the ministers introducing the Bill

were from Labour. More generally, however, political affiliation is less important for explaining the level of understanding of the implications of the proposals than whether the person was speaking in the House of Commons or House of Lords. This pattern was also found in the previous debates about the Regulation of Investigatory Powers Act (Hosein & Whitley, 2002).

Also like the previous debates over the RIP Act, most of the opposition to the Bill arose in the House of Lords. This higher chamber is less party political: many Peers do have party affiliations but they are not as bound by the position of the Party leadership in the Commons, nor is the Labour Party majority as substantial in the House of Lords as in the Commons. Also there are "cross-benchers" in the Lords who have no party affiliation and as such their votes could sway the vote results. Based on the authors' experiences in monitoring national security and law enforcement policies' progress through Parliament, the House of Lords is usually the greater check and balance on the Majority Government.

4.1. What is the retention of communications data?

The ways in which various discourses shape or attempt to shape debate is nicely illustrated by the parliamentary debates about the retention of communications data. Much care was taken by government spokespersons to emphasise the uncontroversial nature of what was being proposed. Lord Rooker, Minister of State at the Home Office, argued:

> [A]ll we are asking for is the retention of the billing detail that any noble Lord would see on a telephone bill; namely, the date a call was made, the number to which it was made, and the time and duration of the call. There is no conversational content in the billing details—indicating that we are not seeking that. We are seeking the billing information ... . This is not an issue of eavesdropping on people's personal correspondence or phone calls, whether they be e-mails or telephone conversations. Effectively we seek only the retention of the billing data (Hansard, 2001e, col. 152).
>
> Only data used for billing purposes—date, time, place, telephone number, period of call—will be retained, not conversations or messages between individuals (Hansard, 2001d, col. 1474).

Yet Lord Rooker also made clear that some of the data that was being requested went slightly further than this:

> It is possible to tell the locations of the mobile phones from which calls are made. That is extremely useful information. They may be mobile, but they are not so mobile as some of the terrorists might think (Hansard, 2001e, col. 152).

There was also concern expressed about the retention of data that does not fit into the standard pattern of the telephone bill, for example, internet access. Lord Phillips of Sudbury commented:

> It is true that the content of telephone conversations and other communications cannot be pried into. However, as is well known in the industry, the "where, when, how, to whom and with whom?" of all communications, the website hits that anyone makes in the course of the daily round, if trawled automatically, enables the state and the "relevant authorities" to build up a personality profile that tells a great deal, in intimate detail, about citizens (Hansard, 2001d, col. 1475).

Over time, the simplified view of communications data as being like a phone bill unravelled, as further complexities were introduced (Law & Mol, 2002). Nevertheless, these statements show how government spokespersons and proponents of the Bill used language to try and frame the debate in non-controversial terms: retaining nothing more than would be seen "on a telephone bill." In the discourse, this data was to be kept for an extended period of time, but also for an extended set of purposes.

Another area where the discourse of government became problematic was in the area of the breadth of powers covered by the Act, and in particular the claimed link between terrorism and organised crime. Parliamentarians often noted that the Bill was intended to be a response to terrorist attacks and to aid in combating terror, and in turn should not be used for other purposes such as combating crime generally. Or more simply put, they argued that an emergency Bill should only address the pressing issue of terrorism, and

not enable mass surveillance for other purposes. This was raised by a number of speakers, including the Earl of Northesk:

> [W]hat need do the Government have of such a broad scope of data retention powers on the face of the Bill? (Hansard, 2001c, col. 954).
>
> None of us disputes that law enforcement should have adequate powers to counter the threat of global terrorism. We all share that aspiration. But those powers should not overreach themselves unnecessarily. As our debates on this issue have demonstrated so visibly, there is widespread concern that that is precisely what the Bill does (Hansard, 2001c, col. 954).

Along the same lines, Lord Phillips of Sudbury argued:

> I shall not take the debate further, except to say that I cannot resist referring to the fact that, at various points during this hurried debate during the past few days, Ministers have expressed indignation at references from this side of the House to the powers of the Bill, taken collectively, to allow trawling and, as I put it in one debate, mass surveillance. Without the restrictions to matters of national security and terrorism, they are precisely that (Hansard, 2001c, col. 971).

These interventions ran the risk of framing future discussion around provocative terms like trawling and mass surveillance, and so David Blunkett, the Home Secretary, clarified the need for broader powers:

> [I]t is impossible to distinguish the issues when one cannot separate out crime and terrorist funding, crime and terrorist organisation, and crime used to fund terrorist acts. That is why there is a provision allowing data already held by the service providers to be held under the voluntary code that we intend to put in place (Hansard, 2001b, col. 37).

The Government was able to transform the concern of creating anti-terrorism powers to combat crime into combating crime because this enables terrorism. The distinction was thus blurred.

4.2. The broad context of the Act

ATCS was introduced and given its first reading on November 12, 2001, barely 2 months after the attacks on the US. The speed with which it was introduced and debated, plus the broad range of topics it covered, led many to suspect that the attacks were used as a blanket reason for introducing a range of measures that had been in preparation by various government departments (Walker & Akdeniz, 2003).

In the House of Commons, Jeremy Corbyn noted:

> The Bill has been rushed through; it is extremely dangerous because it is a denial of civil liberties. If we parade ourselves as a democratic society, in times of difficulty it is important to show the rest of the world that we are prepared to stand up for the civil liberties and rights which we enjoy … . My hon. Friends and I are not prepared to support it because it is a dangerous departure from the norm of a Labour party and a labour movement that defends the right to civil liberties in our society (Hansard, 2001a, col. 1120).

Much of the debate continued to be framed in terms of rushed legislation. Lord McNally referred to the proposed legislation as "a perfect example of sweeping up and shelf clearing to grab new powers" (Hansard, 2001e, col. 161). In the House of Commons, Douglass Hogg argued:

> Most of the Bill has simply come out of the Home Office's back lobby. It has a lot of stuff that it wants to put before Parliament, and it has attached it to this Bill. Part 5 deals with incitement to religious hatred, which is a very important issue, but it has nothing to do with terrorism; part 10 on police powers, ditto; part 11 on retention of communications data, ditto; part 12 on bribery and corruption, ditto; part 13 on implementation of the European Union third pillar, ditto. All those matters are important, but they are certainly not about terrorism, and yet we are subjecting them to a very tight timetable (Hansard, 2001b, col. 94).

4.3. Previous legislation: RIPA and the Human Rights Act

The aim of the Code was simply to require communications providers to retain data that could, if needed, be used by government bodies. There was already legislation in place that provided the mechanisms for accessing this data in the form of Regulation of Investigatory Powers Act of 2000 (RIPA). In addition, in common with many pieces of legislation, the Code drew upon existing definitions of, for example, Communications Data (which it took as having the same meaning as in Chapter II of Part 1 of RIPA). Thus the discourse in parliament was already determined, in part, by the previous debates that had taken place and the previous definitions that were now enshrined in law. As Lord McNally stated: "I believe that some of us will recognise old friends and old arguments from the debate on the Regulation of Investigatory Powers Act" (Hansard, 2001e, col. 161).

Elsewhere, the government spokesperson Lord Rooker stated:

> All the powers used will be fully in line with the European Convention on Human Rights and the Regulation of Investigatory Powers Act. There will be no generalised expeditions; they will all be related to specific inquiries and will conform to the terms of the legislation (Hansard, 2001e, col. 152).
>
> I must remind noble Lords that the data will be retained not by the Government but by the communications providers. The provisions do not extend the access powers agreed by Parliament 18 months ago in the Regulation of Investigatory Powers Act, which are also compatible with human rights legislation (Hansard, 2001d, col. 1474).

A conflict of legislation arose, however. ATCS 2001 was passed under concerns of terrorism, and allowed for retention of communications data by service providers. Yet access to this data was legislated by RIPA, allowing access by numerous government agencies in the prevention, detection, or investigation of any crime. That is, a law passed to combat terror shortly after terrorist attacks is usable only under a prior law passed to investigate any suspicious activity. The general public and the government were made painfully aware of this conflict when the Home Office tried to expand the number of agencies who could access traffic data under RIPA in the summer of 2002, leading to a significant public backlash and an apology from the Home Secretary (Assinder, 2002).

5. Arena 2: the discourse of international policy dynamics

The UK policy on retention may be seen from a larger perspective, including international policy dynamics (Escudero-Pascual & Hosein, 2004; Hosein, 2004). At the levels of inter-governmental organisations, regional and community laws and policies, and international diplomacy, retention was pushed, promoted and modelled as fora were shifted and influenced.

In August 2000, a number of UK law enforcement agencies submitted a proposal to the Home Office to require the retention by a central government authority of communications traffic data for up to 7 years, as such information might be useful for investigations (Gaspar, 2000). The public response to this idea was intense and the proposal was withdrawn on grounds of civil liberties and regulatory burdens (Ward, 2001). Also, only a month earlier the UK government had managed to pass RIPA after much controversy (Ward, 2000). The time was not right for further national deliberation on the issue.

In the meantime, international fora were busy at work on the issue. The Council of Europe considered including data retention in its Convention on Cybercrime, but according to discussions between the authors and government negotiators, behind closed doors, and on grounds of privacy and regulatory burdens, this was rejected. Meanwhile, the idea was being promoted at the Group of 8. The G8 was arguing that countries must harmonise their laws to avoid becoming "safe havens" for criminality; law enforcement powers of access to traffic data and retention were considered essential to this goal. After meetings with industry, however, retention was considered impractical and in the summer of 2001 this proposal was effectively abandoned (G8 Government-Industry Workshop, 2001).

A key obstacle to data retention at the G8 and the Council of Europe was the existence of privacy law and data protection regulations. Data retention is contrary to privacy law, particularly in the EU data protection directives of 1995 (European Union, 1995) and 1997 (European Union, 1997). Under these directives, any

traffic data that is not required for billing or engineering purposes must be deleted. This was preventing any progress on implementing data retention in the member states. An opportunity arose to revisit this obstacle to retention when the EU began work on "updating" its data protection directives to cater for electronic commerce and transactions in 2001, which eventually resulted in a 2002 Directive (European Union, 2002).

In October 2001, President George W. Bush wrote a letter to the President of the European Commission recommending changes in European policy, to "(c)onsider data protection issues in the context of law enforcement and counterterrorism imperatives," and as a result to "(r)evise draft privacy directives that call for mandatory destruction to permit the retention of critical data for a reasonable period" (Bush, 2001). This was building from previously articulated concerns that "(d)ata protection procedures in the sharing of law enforcement information must be formulated in ways that do not undercut international cooperation" (US Government, 2001a) and earlier of recommendations to the European Commission working group on cybercrime, including that:

> Any data protection regime should strike an appropriate balance between the protection of personal privacy, the legitimate needs of service providers to secure their networks and prevent fraud, and the promotion of public safety (US Government, 2001b)

Very similar language later appeared in the G8 documents from the May 2002 ministerial meeting regarding data retention (and industry was not invited this time). G8 ministers were calling upon themselves to:

> Ensure data protection legislation, as implemented, takes into account public safety and other social values, in particular by allowing retention and preservation of data important for network security requirements or law enforcement investigations or prosecutions, and particularly with respect to the internet and other emerging technologies (G8 Justice and Interior Ministers, 2002).

Consequently, some inventive language emerged from the EU process of "updating" the privacy directive, *permitting* member states to *allow* for data retention (European Union, 2002). The new data protection directive on electronic services was finalised in the summer of 2002.

The EU 2002 Directive *permitted* countries to pass retention laws; and countries did as well as they could. Justice and Home Affairs Ministers of the EU knew that this would not be enough, however, because the policy landscape across Europe would be fragmented, where some countries have retention, others do not, and even the retention periods vary. Immediately after the 2002 Directive was settled, the Council of the European Union Ministers of Justice and Home Affairs developed a draft Framework Decision on data retention (European Council, 2002). A "framework decision" is a binding document, and would *require* all member states to have policies requiring retention. Such a decision would generate "pressure" on countries whose governments had not yet managed to pass retention policies through their parliaments. The pressure to create a binding and harmonising measure intensified after the bombings in Madrid in March 2004.[4] This pressure seemed to emerge mostly from the UK Home Office (Tempest, 2004). In April 2004, with pressure from the French, Irish, Swedish and British governments, the Framework Decision was re-introduced, calling for a mandatory 3-year retention policy in all Member States by June 2005 (Council of the European Union, 2004).

Therefore, under these international dynamics, data retention went from something that was considered impractical and legally hazardous, to a regime that must be established to combat terror and organised crime, and, in order to address questions of harmonisation, must be established throughout Europe.

6. Arena 3: the regulatory discourse

Whereas the discourse in the UK parliament is freely accessible through online copies of *Hansard*, the discourse from business players is more difficult to access. Therefore, this section will focus on the debate as articulated in the UK consultation process and its responses, as well as the submissions to the Parliamentary All Party Internet Group (APIG, 2002).

[4]And again after the bombings in London in July 2005. Indeed, as we are correcting these proofs the Home Secretary is urging the EU justice and Home Affairs council to implement compulsory communications data retention across Europe.

The business community, and those who represent and relay industry concerns, provided a substantial amount of the responses to these consultation processes. These responses arose from individuals, particular companies (e.g., BT and Microsoft) and from trade organisations and other bodies (e.g., European Information Society Group (EURIM), Internet Service Providers Association (ISPA), Foundation for Information Policy Research (FIPR), etc.).

The Home Office consultation paper sought to shape the debate by carefully presenting an upfront rebuttal to one of the main counter-arguments to retention, namely existing data protection legislation. Under Fair Information Practices (c.f. US Department of Health Education & Welfare, 1973) and enshrined in data protection legislation (HMSO, 1998a) organisations should only use data for the purposes it is collected for and only keep it for the period that it is needed for that purpose. Often privacy legislation is seen as a regulatory burden on industry; but calling on industry to retain these records introduces a new regulatory burden, and arguably a greater one.

The Home Office also sought to reframe the debate over the legality of retention. In accordance with the Human Rights Act 1998 (HMSO, 1998b), all interventions by government must be "proportionate" to the legitimate aims being pursued. The Home Office argued that the (new) retention periods were indeed proportionate, where proportionality is explained in terms of: degree of intrusion, strength of public policy justification and adequacy of safeguards to prevent abuse (Home Office, 2003a).

The effect of this shaping of the discourse can be seen in part of the oral evidence given by FIPR:[5]

> On forcing ISPs and telephone companies to retain that data for longer than (they) already do for business purposes, we think, is a *disproportionate invasion of privacy* (emphasis added)(Brown, 2002)

FIPR grounded its assessment of "proportionate" on the lack of adequate safeguards and oversight, weak authorisation procedures, the intrusiveness of the data sought, and the burdens upon industry particularly if service providers are compelled to collect additional information.

The main concerns raised by the respondents revolved around three issues: the costs to business of implementing the code of practice, the retention timescales (which have a direct impact on the costs) and the voluntary nature of the Code.

Evidence from AOL in the UK suggests that they currently record details on about 296 million sessions each day (AOL, 2002). This is the equivalent of 100 CDs of data per day, or 36,500 CDs per year (De Stemple, 2002). The business community clearly recognises the enormous costs associated with storing this data for extended periods and these costs increase markedly if the authorities seek to search for particular data within this retained archive. They cannot simply hand over the 36,500 disks, as this would clearly invalidate any reasonable understanding of proportionality.

Industry also raised the issue of the costs of putting in place suitable systems to handle requests for retained data (ISPA, 2002). Large ISPs have full-time staff handling requests, whereas smaller ISPs do not have this capability and need to devote valuable senior management time whenever requests are received. In addition, the fact that the data was being held would increase the likelihood of requests being made. Making the proposals compulsory would, at least, level the competitive playing field in this area. However, it was argued, this would also impose significant barriers to new entrants into the marketplace and would affect competition (ISPA, 2002).

Calculating the costs to industry was not easy, particularly as the practice was unprecedented and there was little experience in managing the projected quantities of data. Extending the period of retention complicates matters greatly, not only due to the storage capacities but also maintaining access facilities. The government promised to set aside some funds to support ISPs with their costs of data retention. In the first year the government promised 4 million GBP, and "future provision will be reviewed in the light of take-up of the code of practice on voluntary data retention by communications service providers" (Hansard, 2003, col. WA148). However, calculating the level of support provided is complicated as some of the data would already be retained for business reasons, and so the government contribution would be intended to cover the marginal costs associated with extending the period the data is held. There were concerns raised about the level of

[5]FIPR is a policy think-tank that works in the technology policy area and seeks to promote better understanding and dialogue between business, government and NGOs across Europe in areas of technology policy.

support provided to the industry as a whole. For example, AOL estimated that it would cost them $40 million to implement retention, and $14 million per annum to maintain the collection, storage, and access facilities (AOL, 2002).

Another concern raised by business was in regards to the risks of having large quantities of data stored, either by government or commercial organisations. Some of these risks arise from simply having data available in one place. As the EURIM (2002) submission suggests:

> Those responsible for security in major international and financial services users are well aware of incidents in recent years where those in national security, law enforcement and other public sector agencies in the US and UK have abused positions of trust for personal gain.

Other problems arise with the processes that are in place for handling this data. Again, from the EURIM (2002) submission:

> Some agencies are known to have internal processes that would not be tolerated by any private sector regulator, let alone a financial services regulator. There are similar issues with regard to some suppliers of security software (including encryption) and services (including technology support).

One particular discourse that was not raised by business, although it would have been of interest to privacy groups, was about the existing use that is made of communications data for marketing and profiling activities. Additionally, little discussion arose regarding how this information could be used for non-criminal investigations, such as after complaints by content-producing industries investigating illegal file sharing. While the former activities would have required substantial re-writing of data protection law, the latter is arguably similar to retention for preventing, detecting, and investigating criminal activities as copyright infringement is illegal. To date, discourses regarding these forms of additional access and processing have not arisen within Europe, much to our surprise. Such discourses have occurred elsewhere, for example in Canada and the US where much controversy has arisen surrounding court cases, though these countries do not have retention policies.

7. Arena 4: the technological discourse

The constitution of traffic data is a contentious discourse of its own. As discussed earlier, much of the discussion in the UK parliament contends that traffic data is merely telephone transaction records. With shifts and developments in technology and infrastructure, traffic data may now include many other forms of communication (e-mail, SMS, instant messaging) and transmission protocols (GPRS, IPv6, etc.). What is captured under the technological discourse depends greatly on the legal definitions.

In the UK, the definition of "communications data" is complex; a result of previous policy battles. The Regulation of Investigatory Powers Act 2000 went through many iterations, particularly in the so-called "Big Browser" debate, before the government acquiesced in the later stages of deliberation (FIPR, 2000). Traffic data is defined there as data about the source and destination of a transaction, and data about the routing and the tying of separate packets together. This definition is complemented by the definition of "communications data" which is data attached to a transaction provided that it is used by the network, or exists within logs, or is otherwise collected by service providers. Under RIPA Part I Chapter II, government agencies have access to communications data held by Communications Service Providers (CSPs). This distinction prevented government agencies from easily gaining access to more sensitive transactional data such as web-browsing habits, qualifying this data as communications content instead.

Other recent initiatives to define communications data have noted the increased breadth of the communications infrastructure. For example, the Group of 8 working-definition of traffic data is:

> [n]on-content information recorded by network equipment concerning a specific communication or set of communications. Traffic data includes the origin of a communication, the duration, the nature of the communication activity (not including content) and its destination. In the case of internet communications, traffic data will almost always include an IP address and port number (G8, 2001).

```
time_GMT=20010810010852 Cell_ID=115 MAC_ID=00:02:2D:20:47:24
time_GMT=20010810010852 Cell_ID=115 MAC_ID=00:02:2D:04:29:30
time_GMT=20010810010854 Cell_ID=129 MAC_ID=00:02:2D:04:29:30
time_GMT=20010810010854 Cell_ID=129 MAC_ID=00:02:2D:20:47:24
time_GMT=20010810010856 Cell_ID=41  MAC_ID=00:02:2D:04:29:30
time_GMT=20010810010856 Cell_ID=41  MAC_ID=00:02:2D:20:47:24
time_GMT=20010810010900 Cell_ID=154 MAC_ID=00:02:2D:20:47:24
time_GMT=20010810010900 Cell_ID=154 MAC_ID=00:02:2D:04:29:30
```

Fig. 3. Wireless access logs.

Meanwhile, the Council of Europe (CoE) Convention on Cybercrime defines traffic data as

> any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service (CoE, 2001).

These differing definitions incorporate increasing amount of data, and personal information. Surprisingly, the G8 and the CoE were negotiated by many of the same officials.[6]

The constitution of communications data differs from communications infrastructure to infrastructure. What is "signalling data" for the telephone system is drastically different for mobile telephony. Consequently, particular data that is associated with communications but that is not content may come close to providing content, or disclose additional information. For some technologies, this may stretch the proportionality argument for retention that was alluded to earlier.

Even the plain old telephone system communications data held in logs can be linked with subscriber information and hence identify the location of the calls being made and received. That is, odds are that you were at home when you made that call, and when you answered that call to your home phone.

Mobile phones take this a step further as they disclose location and changes in location during a call. Connecting to an internet service provider often involves a modem connection that includes a source telephone number which may change as users roam nationally or internationally, connecting to global service providers.

Connecting to servers whilst on the internet leaves transaction records of internet addresses which may be traced back to a specific user, location, and time. Logs from wireless networks can link particular cells (physical locations) with MAC IDs (particular machines). They therefore contain more than just which machine connected to the network when and can also be automatically analysed to see who else was present at that location. For example, from Fig. 3, we can see that two machines were co-located at Cell 129 at a particular time.

Further problems arise with TCP/IP and application traffic data. The retention proposals call for web activity logs to be kept for 4 days, storing information that is "restricted solely to communications data and exclude content of communication. This will mean that storage under this code can only take place to the level of www.homeoffice.gov.uk/…" (Home Office, 2003c, Appendix 1). This assumes, of course, that particular websites are uniquely identified by their top name. Thus, a user who browses http://www.homeoffice.gov.uk/terrorism/index.html and http://www.homeoffice.gov.uk/crimpol/index.html is visiting the "same" Home Office website. In other cases, however, many top-level sites "host" many individual sites. For example, Geocities http://geocities.yahoo.com/ allows you to create your own mini site from this name. Presuming that law enforcement wants to know which of these individual sites are being accessed rather than just Geocities' servers, data will need to be retained beyond the top level. This, however, leads to practical problems of differentiating between http://geocities.yahoo.com/edgarwhitley which is communications data and http://www.google.co.uk/search?q=edgar+whitley which contains content data (the search items).

[6]Traditionally, international agreements are arranged for by Foreign Ministries. In the negotiation of the G8 and the CoE agreements, however, the Ministries of Justice and Home Affairs were usually the only government representation in the room. The authors worked closely with a number of Government officials in various countries, and the two initiatives were often inseparable in discussions. The authors also attended a number of meetings in each institution, and kept on running in to the same officials.

Communications data can disclose a large amount of information regarding individuals, even where there are safeguards. When requesting information from www.aidshelp.org the uniform resource locators (URLs) may also qualify as header data to TCP packets, but may not be logged on a regular basis. Moreover, under UK law, URLs are considered communications content and thus require a warrant authorised by the Secretary of State. However, interactions with a server 209.25.215.42 (which can be resolved to be www.aidshelp.org) may disclose just as much information regarding interests and concerns of the individual, and all this information is being collected indiscriminately. More problems will arise with the next generation internet, as mobility bindings or routing information are included in the IPv6 extended header that will include location information (Escudero-Pascual & Hosein, 2004), making already sensitive communications data even more so.

8. Conclusions

This section begins by tracing the likely developments in the retention of communications data in the UK, and implications for understanding policy. It then reviews some of the contributions to methodology that this study has presented.

8.1. Likely developments

Now that the ATCS is law, and the Code of Practice was approved by parliament, the final test for the UK policy on data retention remains its compliance with the Human Rights Act 1998 (HMSO, 1998b). The HRA requires that all laws in the UK are consistent with the European Convention on Human Rights (ECHR) (CoE, 1950) and associated jurisprudence. In particular, article 8 guarantees the individual's right to privacy. No one has, to date, taken the case to the courts, but non-governmental organisations and other actors have sought legal advice on the matter.

According to the ECHR, any invasion of privacy must be in accordance with law and necessary in a democratic society. In accordance with jurisprudence, "necessary in a democratic society" means that the laws must be in response to a pressing social need and proportionate to the aim pursued. Similarly derived, "in accordance with law" means that the law must be accessible to the public, reasonably precise, and not allow for the unfettered exercise of discretion (European Court of Human Rights, 1980). The European Court of Human Rights has previously ruled that interception of communications created "a menace of surveillance" for all users, striking at freedom of communication and thus was an invasion of privacy (European Court of Human Rights, 1980). Similarly, retention is arguably an invasion of privacy as it threatens all users of communications services with the menace that either public or private actors will abuse the records made.

The legal intrusion on individual privacy will be more invasive as the technology continues to permeate society. A key requirement to assessing whether an invasion is in accordance with law is that the law should at least be "foreseeable". That is, laws should be written in such a way that individuals should be able to regulate their conduct accordingly, so as to avoid invoking unwelcome intrusions. Increasingly, all that we do in our daily lives involves some form of communications transaction. In so doing, we are subjecting ourselves to surveillance by default, as our activity is retained indiscriminately, preventing us from avoiding such surveillance. As legal experts conclude, "blanket data retention would subject every citizen to the certainty of ongoing and unremitting interference in his or her private life" (Privacy International, 2003).

As the likely constitutional implications of data retention are considered, it becomes clear that this is not just a legal issue. Assessing the legality of the law requires investigation beyond merely legal constructs such as the letter of the legislation, into the other discourses. Foreseeability can only be measured by understanding the expansive nature of the technology and the future patterns of market structures. Proportionality can only be understood by looking at the business costs and regulatory impacts, while also understanding the constitution of "communications data". Thus even something as apparently clear as legislation is inextricably intertwined with the other discourses presented in this paper: technological, regulatory, and parliamentary. The point here is not that these discourses are discrete. Rather, the paper argues that these varied discourses exist, and secondly and most importantly, that when they are brought together a deeper appreciation of the politics of technology policy is possible.

This approach can be used to understand the potential implications to changes in US law. The US has not pursued data retention as a domestic policy in the area of communications data. However, the US would appear to be adopting an alternative strategy to the question of introducing the technological into politics, by attempting to have technology-neutral policy. The constitutional protection of communications data in the US is nil, as decided in *Smith V. Maryland*.[7] In this case, the Supreme Court decided that there was no reasonable expectation of privacy in this area.

In response to that ruling, the Electronic Communications Privacy Act of 1986 raised the requirements for access to traffic data, requiring a court order for access to this information, where authorisation is received if the information "is relevant to an ongoing investigation". Meanwhile the Cable Act of 1984 protects cable data to a degree greater than communications content ("clear and convincing evidence" rather than "probable cause").

The legal landscape was transformed by the USA-PATRIOT Act. First the Act amended the wiretap laws under Title III to include internet technology, "updating" older language to include language similar to the G8 definitions discussed earlier. Secondly, the Cable Act was amended to allow government access more in-line with ECPA when cable companies provide internet services to their customers. This "technology-neutral" approach was lauded by Attorney General John Ashcroft:

> Agents will be directed to take advantage of new, technologically neutral standards for intelligence gathering … . Investigators will be directed to aggressively pursue terrorists on the internet. New authority in the legislation permits the use of devices that capture senders' and receivers' addresses associated with communications on the internet (Ashcroft, 2001).

By treating all data equally, however, the assumption is made that all technologies can be treated equally. This attempt to reduce the technological to a non-problematic discourse is likely to have political and regulatory ramifications such as concerns regarding "Big Brother" and costs to small business, respectively. These concerns may emerge once challenged in the US courts on constitutional grounds. There the courts may revise their earlier assessment that communications data does not deserve protection under the US Constitution, particularly when consideration is given to how much information can be gathered by looking at the technological discourse. Similarly, accessing communications data from internet service providers is not as easy as it was with telephone companies because of the availability of this data and its collection and maintenance, and so the effects on business will only be understood after investigating the technological discourse.

For example, Kerr (2003, p. 655), when describing why the FBI's Carnivore[8] interception system is "generally more privacy enhancing than other less sophisticated pack sniffers in everyday use at ISPs" states that "Emails are identifiable because a section of the packet header contains an identifying number that lets the server know that the packet should be sent to the mail server. To be technical, emails are carried on port 25, which means the sniffer can just look for communications sent to port 25" (Kerr, 2003, footnote 206). As such, this definition will fail to address web-based email services such as hotmail and will either potentially miss out on a large number of email messages or will need to be adapted to include such messages (which are difficult to separate from other http traffic). Consequently this definition will face many of the problems foreseen in the parliamentary debates about RIPA (Hosein & Whitley, 2002).

8.2. Methodological contributions

This article has argued that the study of policy discourse is an effective way to understand the complexities associated with the development of policy surrounding the retention of communications data in the UK. It first proposed that there exist discourses in four arenas and in turn that, by looking at all of these discourses,

[7]Smith V. Maryland (1979) 442 U.S. 735, 742.

[8]Carnivore is a surveillance device used by the US Government to conduct surveillance at internet service providers. It is attached to the ISP's network and it scans all traffic to identify the packets for an individual suspect. Much controversy has arisen regarding this system, and it has been renamed DCS 1000. For more information see (Electronic Privacy Information Center & Privacy International, 2004).

better understanding of the policy, and in particular, its legality can be gained. This section reviews some of the methodological contributions of this approach. These contributions lie in three areas: the micro/macro-distinction and the strength of boundaries between discourses; the effectiveness of different discourses in shaping debate; and the representation of technological concerns.

One of the benefits of discourse analysis is that the level of discourse moves seamlessly between the macro and the micro. In many social science approaches it is common to use different analytical techniques for different levels of analysis (Callon & Latour, 1981). However, the approach used in this paper does not encourage such artificial separation of levels as the same legislation can be seen in terms of interventions from the President of the US and international bodies like G8 and Council of Europe, as well as micro level interventions in terms of particular debates that have taken place in the UK parliament. As such it provides a generalisable means of describing the system of action shaping public policy (Dutton, 1992).

Further blurring of boundaries occurs when understanding is sought of these discourses, as the concerns of parliamentary, business, international policy dynamics and technological discourses blend together. For example, understanding business concerns requires an understanding of regulatory and technological factors. Parliament's discourse involves legal and technological factors, as well as some political deliberation (e.g., APIG) that also considers industry concerns and regulatory burdens. To understand the international policy dynamics one has to consider regulatory language such as "harmonisation", jurisdictional arbitrage, and safe havens; while also considering government deliberation processes and concerns. Inclusion of these discourses within this research is necessary, even when they do not arise naturally. A study of regulatory aspects to the internet must consider the technological alongside the social aspects. A study of parliamentary attitudes to electronic commerce, in turn, also requires discussion of international issues.

In turn, a more complete understanding of the legal contentions requires a better understanding of the surrounding discourses. To appreciate the legal burden of retention it is necessary to look at the business discourse to appreciate what is proportional. To understand why national privacy law no longer prevents data retention, international policy dynamics must be considered. To understand why despite the legal problems, the conflict with privacy law, and the regulatory costs, the ATCS 2001 and its Code of Practice were approved, parliamentary discourse is a target for analysis.

This article has also shown how language and discourse is used to attempt to shape the development of policy. Language is continuously negotiated, with such terms as "proportionality" and "communications data" being interpreted differently depending on political goals. Proportionality was held up to defend the Bill and to attack it; "communications data" was implicitly and explicitly defined both trivially (as telephone data) and in detail (as a map of human activity). Watching how the language is negotiated and the transformations in the discourses allows the achievement an in-depth view of how the policy formed.

The language-based analysis of this paper also draws (or rather removes) another methodological distinction, namely between language about human actions (such as the effects of the legislation on human rights) and language about non-humans. Whilst the first is recognised as unproblematic, the evidence in this article shows how people are equally capable of talking on behalf of business "concerns" or about the technology.

The study of the retention of communications data in the UK therefore demonstrates the complexities of understanding the development and implementation of telecommunications policies in areas where the technological plays an increasingly important role. Other discourses that exist simultaneously, including the regulatory, parliamentary, and geo-political discourses were also identified. In the UK case, the parliamentarians, particularly in the House of Lords, have been prepared to learn about the capabilities of the technology, to allow them to engage in debate with technologists and business; but all this discussion may be subverted by developments at the EU. Industry organisations would need to lobby both parliament and international institutions simultaneously, which some did with some success. Finally, more effective mechanisms for making the technological a part of our policy deliberations are needed. In drawing attention to this, the paper is explicitly calling for the kind of abnormal policy discourse across communities of practice advocated by Throgmorton.

References

Akdeniz, Y., Taylor, N., & Walker, C. (2001). BigBrother.gov.uk: State surveillance in the age of information and rights. *Criminal Law Review*, *February*, 73–90.

Akrich, M. (1992). The de-scription of technical objects. In W. E. Bijker, & J. Law (Eds.), *Shaping technology/building society: Studies in sociotechnical change* (pp. 205–224). Cambridge, MA: The MIT Press.

AOL. (2002). *AOL evidence to APIG*, at http://www.apig.org.uk/Data%20Retention%20APIG.doc.

(APIG) Parliamentary All Party Internet Group. (2002). *Data retention enquiry*, at http://www.apig.org.uk/publications.htm.

Ashcroft, J. (2001). *Prepared remarks for the US Mayors conference*. Washington, DC: US Congress at http://www.yale.edu/lawweb/avalon/sept_11/doj_brief020.htm.

Assinder, N. (2002). Blunkett abandons Big Brother. *BBC News Online,* June 18, at http://news.bbc.co.uk/1/hi/uk_politics/2051670.stm.

Baumgartner, F. R., Jones, B. D., & Wilkerson, J. D. (2002). Studying policy dynamics. In F. R. Baumgartner, & B. D. Jones (Eds.), *Policy dynamics* (pp. 29–46). Chicago: University of Chicago Press.

Boland, R. J., & Tenkasi, R. V. (1995). Perspective making and perspective taking in communities of knowing. *Organization Science*, *6*(4), 350–372.

Brown, I. (2002). *FIPR oral evidence*, at http://www.apig.org.uk/fipr_oral_evidence.htm.

Bush, G. W. (2001). *Letter from President George W. Bush to Mr. Romano Prodi, President, Commission of the European Communities*. Brussels: Forwarded by the Deputy Chief of Mission to the European Union, October 16, at http://www.statewatch.org/news/2001/nov/06Ausalet.htm.

Callon, M., & Latour, B. (1981). Unscrewing the big leviathan: How actors macro-structure reality and how sociologists help them do so. In K. Knorr-Cetina, & A. Cicourel (Eds.), *Advances in social theory and methodology* (pp. 277–303). Boston: Routledge & Kegan Paul.

Council of Europe Convention (CoE). (1950). *European Convention on Human Rights*, at http://conventions.coe.int/treaty/en/Treaties/Html/005.htm.

Council of Europe Convention (CoE). (2001). *Council of Europe, Convention on Cybercrime, ETS 185, Opened for Signatures November 2001,* at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

Council of the European Union. (2004). *Draft framework decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism*. Brussels: From the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom at http://www.ispai.ie/fd.pdf.

Crane, R. J. (1978). Communications standards and the politics of protectionism. *Telecommunications Policy*, *2*(4), 267–281.

De Stemple, C. (2002). *ISPA/AOL oral evidence*, at http://www.apig.org.uk/ispa_oral_evidence.htm.

Dutton, W. H. (1992). The ecology of games shaping telecommunications policy. *Communications Theory*, *2*(4), 303–328.

Electronic Privacy Information Center and Privacy International (EPIC). (2004). *Privacy and human rights 2004: An international survey of privacy laws and developments*. Washington, DC: Electronic Privacy Information Center.

Escudero-Pascual, A., & Hosein, I. (2004). Questioning lawful access to traffic data. *Communications of the ACM*, *47*(3), 77–82.

European Council. (2002). *Draft framework decision on the retention of traffic data and on access to this data in connection with criminal investigations and prosecutions*. Brussels: EU.

European Court of Human Rights. (1980). *Klass v. Germany* (no. 2 European Human Rights Report 214).

European Information Society Group (EURIM). (2002). *Written evidence to APIG*, at http://www.apig.org.uk/eurim.pdf.

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* (No. Official Journal L281).

European Union. (1997). *Directive 97/66/EC of the European Parliament and the council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector* (No. Official Journal L24).

European Union. (2002). *Directive 2002/58/EC of the European parliament and of the council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications)* (No. Official Journal L201).

Foundation for information policy research (FIPR). (2000). *RIP Bill in Parliament*, at http://www.fipr.org/rip/parliament.html.

G8. (2001). US delegation. *Discussion paper for data preservation workshop. G8 conference on high-tech crime*, Tokyo, May 22–24, 2001.

G8 Government-Industry Workshop. (2001). *Report from data preservation workshop*. Group of 8 Conference on High-Tech Crime, Tokyo.

G8 Justice and Interior Ministers. (2002). *G8 statement on data protection regimes*.

Gaspar, R. (2000). *Looking to the future: Clarity on communications data retention law; a submission to the home office for legislation on data retention*: On behalf of ACPO and ACPO(S); HM Customs and Excise; Security Service; Secret Intelligence Service; and GCHQ, at http://www.statewatch.org/news/dec00/02ncis.htm.

Hansard. (2001a). House of Commons December 13, 2001 (Commons consideration of Lords reasons and amendments).

Hansard. (2001b). House of Commons, November 19, 2001 (Second Reading).

Hansard. (2001c). House of Lords, December 6, 2001 (Report stage).

Hansard. (2001d). House of Lords, December 13, 2001 (Lords consideration of Commons reason and amendment).

Hansard. (2001e). House of Lords, November 27, 2001 (second reading).

Hansard. (2003). *House of Lords October 20, 2003 on anti-terrorism, crime and security Act 2001: Retention of communications data.* House of Lords.

HMSO. (1998a). *Data Protection Act 1998*, at http://www.hmso.gov.uk/acts/acts1998/19980029.htm.
HMSO. (1998b). *Human Rights Act 1998*, at http://www.hmso.gov.uk/acts/acts1998/19980042.htm.
HMSO. (2000a). *Regulation of Investigatory Powers Act 2000*, at http://www.opsi.gov.uk/acts/acts2000/20000023.htm.
HMSO. (2000b). *Terrorism Act 2000*, at http://www.hmso.gov.uk/acts/acts2000/20000011.htm.
HMSO. (2001a). *Anti-Terrorism, Crime and Security Act 2001*, at http://www.legislation.hmso.gov.uk/acts/acts2001/20010024.htm.
HMSO. (2001b). *Anti-Terrorism, Crime and Security Act 2001, Part 11*, at http://www.legislation.hmso.gov.uk/acts/acts2001/10024–l.htm#102.
Home Office. (2003a). *Access to communications data respecting privacy and protecting the public from crime*, at http://www.homeoffice.gov.uk/docs/consult.pdf.
Home Office. (2003b). *Consultation paper on a code of practice for voluntary retention of communications data*, at http://www.homeoffice.gov.uk/docs/vol_retention.pdf.
Home Office. (2003c). *Retention of communications data under Part 11: Anti-terrorism, crime and security Act 2001*, at http://www.legislation.hmso.gov.uk/si/si2003/draft/5b.pdf.
Hood, C. (1994). *Explaining economic policy reversals*. Buckingham, England: Open University Press.
Hosein, I. (2002). A research note on capturing technology: Towards moments of interest. In E. H. Wynn, E. A. Whitley, M. D. Myers, & J. I. DeGross (Eds.), *Global and organizational discourse about information technology* (pp. 133–154). Boston: Kluwer Press.
Hosein, I. (2004). The sources of laws: Policy dynamics in a digital and terrorized World. *The Information Society*, *20*(3), 187–199.
Hosein, I., Tsiavos, P., & Whitley, E. A. (2003). Regulating architecture and architectures of regulation: Contributions from information systems. *International Review of Computing Law and Technology*, *17*(1), 85–97.
Hosein, I., & Whitley, E. (2002). The regulation of electronic commerce: Learning from the UK's RIP Act. *Journal of Strategic Information Systems*, *17*(1), 31–58.
Introna, L. D. (1997). *Management, information and power: A narrative of the involved manager*. Basingstoke: Macmillan.
Internet Service Providers Association (ISPA). (2002). *ISPA oral evidence*, at http://www.apig.org.uk/ispa_oral_evidence.htm.
Kerr, O. S. (2003). Internet surveillance law after the USA Patriot Act: The big brother that isn't. *Northwestern University Law Review*, *97*(2), 607–673.
Kingdon, J. (1995). *Agendas, alternatives, and public policies* (2nd ed.). New York: Harper Collins.
Latour, B. (2000). When things strike back: A possible contribution of 'science studies' to the social sciences. *British Journal of Sociology*, *51*(1), 107–123.
Latour, B. (2004). *The politics of nature: How to bring the sciences into democracy (C. Porter, Trans.)*. Cambridge, MA: Harvard University Press.
Law, J., & Mol, A. (Eds.). (2002). *Complexities: Social studies of knowledge practices*. Durham: Duke University Press.
Majone, G. (1989). *Evidence, argument, and persuasion in the policy process*. New Haven: Yale University Press.
Mlcakova, A., & Whitley, E. A. (2004). Configuring peer-to-peer software: An empirical study of how users react to the regulatory features of software. *European Journal of Information Systems*, *13*(2), 95–102.
Mosco, V. (1988). Toward a theory of the state and telecommunications policy. *Journal of Communication*, *38*(1), 107–124.
Orlikowski, W. J., & Iacono, C. S. (2001). Research commentary: Desperately seeking the "IT" in IT research: A call to theorizing the IT artifact. *Information Systems Research*, *12*(2), 121–134.
Pouloudi, A., & Whitley, E. A. (1997). Stakeholder identification in inter-organizational systems: Gaining insights for drug use management systems. *European Journal of Information Systems*, *6*(1), 1–14.
Pouloudi, A., & Whitley, E. A. (2000). Representing human and non-human stakeholders: On speaking with authority. In R. Baskerville, J. Stage, & J. I. DeGross (Eds.), *Organizational and social perspectives on information technology* (pp. 339–354). Aalborg, Denmark: Kluwer.
Privacy International. (2003). *Memorandum of laws concerning the legality of data retention with regard to the rights guaranteed by the European convention on human rights*. London: Convington and Burling at http://www.privacyinternational.org/issues/terrorism/rpt/data_retention_memo.pdf.
Rein, M., & Schön, D. (1993). Reframing policy discourse. In F. Fischer, & J. Forester (Eds.), *The argumentative turn in policy analysis and planning* (pp. 145–165). Durham, NC: Duke University Press.
Stigler, G. (1983). Nobel lecture: The process and progress of economics. *The Journal of Political Economy*, *91*(4), 529–545.
Streeter, T. (1990). Beyond freedom of speech and the public interest: The relevance of critical legal studies. *Journal of Communication*, *40*(2), 43–63.
Suchman, L. A. (1987). *Plans and situated actions: The problem of human–machine communication*. Cambridge: Cambridge University Press.
Tempest, M. (2004). Blunkett attacks EU 'waffle' on security. *The Guardian*, March 19th, at http://politics.guardian.co.uk/attacks/story/0,,1173516,00.html.
Throgmorton, J. (1991). The rhetorics of policy analysis. *Policy Sciences*, *24*(2), 153–179.
Tyler, M. (1979). Videotext, Prestel and Teletext: The economics and politics of some electronic publishing media. *Telecommunications Policy*, *3*(1), 37–51.
US Department of Health Education and Welfare. (1973). *Records, computers, and the rights of citizens: Report of the secretary's advisory commission on automated personal data systems*. US Government.
US Government. (2001a). *Comments of the United States government on the European commission communication on combating computer crime*, Brussels.

US Government. (2001b). *Prepared statement of the United States of America, presented at European Union Forum on Cybercrime*, at http://www.cybercrime.gov/intl/MMR_Nov01_Forum.doc.

Walker, C., & Akdeniz, Y. (2003). Anti-terrorism laws and data retention: War is over? *Northern Ireland Legal Quarterly*, *54*(2), 159–182.

Ward, M. (2000). 'Snooping' bill protests stepped up. *BBC News Online,* July 12, at http://news.bbc.co.uk/1/hi/sci/tech/830318.stm.

Ward, M. (2001). Government 'snoop law' stance slammed. *BBC News Online,* May 17, at http://news.bbc.co.uk/1/hi/sci/tech/1335963.stm.

Woolgar, S. (2002). *Virtual society? Technology, cyberbole, reality*. Oxford: Oxford University Press.

Wu, I. (2004). Canada, South Korea, Netherlands and Sweden: Regulatory implications of the convergence of telecommunications, broadcasting and Internet services. *Telecommunications Policy*, *28*(2), 79–96.

Wynn, E. H., Whitley, E. A., & Myers, M. D. (2003a). Placing language in the foreground: Themes and methods in information technology discourse. In E. H. Wynn, E. A. Whitley, M. D. Myers, & J. I. DeGross (Eds.), *Global and organisational discourse about information technology* (pp. 1–12). Boston: Kluwer.

Wynn, E. H., Whitley, E. A., Myers, M. D., & DeGross, J. I. (Eds.). (2003b). *Global and organisational discourse about information technology*. Boston: Kluwer.

Yanow, D. (1996). *How does a policy mean? Interpreting policy and organizational actions*. Washington, DC: Georgetown University Press.

Yen, J. (Ed.), (2004). Special section: Emerging technologies for homeland security. *Communications of the ACM*, *47*(3), 32–69.