NILQ 69(1): 59–84

(Re)conceptualising state secrecy

Lydia Morgan

Birmingham Law School, University of Birmingham

Abstract

This paper seeks to reconceptualise state secrecy and asks whether it is adequately understood in the UK. It argues that state secrecy is systemic not exceptional and that it is supported by complex institutional structures and cultural practices. It analyses the legislative armoury of state secrecy, including investigatory powers (RIPA, DRIPA and IPA) and develops a tripartite model of state secrecy. Properly understood, state secrecy can be divided into three categories: esoteric, operational and efficient. Esoteric state secrecy restricts access to decision-making and information. It is a facet of power, utilised to control. Operational state secrecy protects techniques, procedures and investigations. It is not as all-encompassing as esoteric state secrecy, but can be cumulative where one demand for secrecy creates another. Finally, efficient state secrecy references the pragmatic sense in which secret conditions allow faster decision-making and the conceptual limits of transparency in a modern complex state. These categories illuminate how state secrecy's true effects are masked because it is so entrenched.

Keywords: Concept of secrecy; state secrecy; national security; public law; investigatory powers; freedom of information; transparency.

Introduction

States keep secrets. While, perhaps, expected, this poses particular challenges in self-defined liberal democracies such as the UK. These challenges become more acute when we recognise that, far from being exceptional, secret-keeping is the cultural mode of British politics. State-level secretive behaviour takes many forms. It is seen in the security services (MI5, MI6, Government Communication Headquarters (GCHQ)); in legislation (the Official Secrets Act 1909–1989 and the Freedom of Information Act (FOI) 2000); in 'national security' closed court hearings; and even in the involvement of the Prince of Wales in government policy formation.[1]

Partly because secrecy is treated as exceptional rather than ordinary, a systematic consideration is missing from the literature. From the perspective of law, this is odd. Secrecy is, after all, a concept with significant legal implications. Secrecy alters criminal procedures and evidential standards, and strains, if not outright overturns, the principle of open justice. It provides expanding investigative powers and a special role for

1 R Craig, 'Black Spiders Weaving Webs: The Constitutional Implications of Executive Veto of Tribunal Determinations' (2016) 79(1) Modern Law Review 166–82.

security-related agencies. Secrecy is used to justify internal as well as external mass surveillance. Even the transparency brought forth by the FOI is in fact couched in the need to protect and conceal information. Policy is developed and shaped behind secrecy's veil. Secrecy forces trust in government into a one-way street. The public must trust they are being governed well, but the public are not reciprocally trusted to scrutinise decision-making processes and outcomes. Not only does secrecy partition the public–government relationship, it also fractures relationships within the institutions of the state. When considered separately, these behaviours and activities can seem to be exceptional or unique to their particular arenas, but taken together they describe a common and accepted idea.

This article addresses, from a legal perspective, the lack of systematic and comprehensive consideration of the concept of secrecy. It is not concerned with disrupting the idea of secrecy, but interrogating the specific concept of state secrecy, that is, secrecy utilised in the service of the state. I argue that, when conceptualised in its fullest form, secrecy is a common, challenging and contentious mode of governing. I explore the question 'What is state secrecy?', explain the limits of existing conceptions and demonstrate the conceptual distinction between secrecy and state secrecy. Properly understood, state secrecy can be divided into three overlapping categories: esoteric, operational and efficient. The three elements should not be approached as detailed taxonomies with hard boundaries, but as models which illuminate the working and practice of state secrecy. Some aspects of secrecy fit within more than one category at a time but appear different cast in the alterative light. *Esoteric* state secrecy restricts access to decision-making and information. It is a facet of power, utilised to control. *Operational* state secrecy protects techniques, procedures and investigations. It is not as all-encompassing as esoteric state secrecy but can be cumulative where one demand for secrecy creates another. Finally, *efficient* state secrecy references the pragmatic sense in which secret conditions allow faster decision-making and the conceptual limits of transparency in a modern complex state. These categories illuminate how state secrecy's true effects are masked because it is so entrenched.

While the post-9/11 counter-terror response marks a distinct intemperate moment in the history of state secrecy, the shape and manner of secrecy in the UK does not only result from reactive shifts. Secrecy is so ingrained that rather than being, as Crossman suggested, 'the English disease'[2] and therefore a curable ailment, it is in fact part of the fabric of British political and legal character. Failure to recognise state secrecy as such means its persistence in an 'open society'[3] is unexplained and its benefits and harms ill-judged.

For political and legal concepts to be useful they must reflect and capture the reality of the thing they denote. Without an accurate definition the full scale of state secrecy and the challenges state secrecy poses to liberal democratic principles like accountability, transparency and individual liberty remain unmapped. Exposing the ingrained role of state secrecy enables the claim to necessity to be properly understood – and its excesses challenged – as well as better regulatory practice to be established. This article will show that, at some level, the poor and partial comprehension of state secrecy is a deliberate and expected consequence of a concept that inhibits examination and relates shadow-worlds with the implications of bureaucracy. The first section examines the various attempts to discuss or define state secrecy, before reviewing what aspects of the legal framework

2 R Crossman, 'The Real English Disease', *The New Statesman* (London, 25 September 1971) 1.

3 K Popper, *The Open Society and its Enemies*, vols1 and 2 (Routledge [1945] 2002).

might aid the search for a fuller understanding in the second. The final section will then present a conception of state secrecy to address the problems raised by existing accounts.

1 The meaning(s) of state secrecy

'At the heart of secrecy lies discrimination of some form, since its essence is sifting, setting apart, drawing lines.' [4]

How does state secrecy differ from secrecy? Secrecy is said to be intentional concealment.[5] As it relates to the communicative nature of sociality, it is relational, requiring a secret holder and a subject against whom the secret is held. Secret-keeping is an active endeavour requiring resources to maintain.[6] Concealment is not simply out of view, undiscovered or accidentally omitted. It implies obfuscation, something unavailable because it has been hidden, encrypted or closed to prevent it from being discovered, deduced or worked out. Mystification is instrumental to secrecy, but there is an epistemic difference between a mystery and a secret. However, since many more people are privy to state secrets, intentionality is less ascribable to the definition.[7] For example, at least 20,000 people directly work for the UK security and intelligence agencies and, even assuming secrecy within and between these agencies, a large number of people will be privy to the secrets they hold. So, while secrecy and state secrecy have in common the practice of *deliberate concealment*, each individual state secret may not have the same agent-driven intention as interpersonal secrets. Rather, concealment happens as a result of an institutional or cultural practice.[8]

Secrets do not occur within a vacuum, a singular homogeneous space. Secrecy requires two forms of space: one within which the secret is held; and another from which the secret is withheld. State secrecy multiplies the spaces because state secrets are kept from a variety of publics: the public enemy (external threat), the revolutionary public (internal threat) and the mandated public (members of the state). Similarly, there is a spatial layering of state secrecy within the bounds of the state apparatus. Withheld information bonds parties together through the confidence of the 'aggressive defence',[9] suggesting state secrecy's power is situated not in the content but in the act of making something secret. Secrecy amplifies, making any information 'somehow essential and significant'.[10] Once revealed, secrets are often paltry and devoid of potency.[11] Derrida, observing the intimate connection between controlling information and political power, explained that those who hold the archive, the collated information, hold authority.[12] But preservation is easily blurred with protection and exclusion, making access to the archive a measure of transparency. This is significant from a bureaucratic perspective, as secrecy can shield against criticism and insulate mistakes to facilitate rectification or camouflage.[13]

4 S Bok, *Secrets: On the Ethics of Concealment and Revelation* (Vintage 1989) 28.

5 Ibid 9.

6 E Shils, *The Torment of Secrecy*, P Moynihan (ed) (Elephant Paperback [1956] 1996) 26.

7 P Galison, 'Removing Knowledge' (2004) Critical Inquiry 31.

8 Bok (n 4) 5; P Major and C Moran, *Spooked: Britain, Empire and Intelligence Since 1945* (Cambridge University Press 2009); D Omand, *Securing the State* (Hurst 2012).

9 G Simmel, 'The Sociology of Secrecy and Secret Societies' (1906) 11(4) American Journal of Sociology 462.

10 Ibid 465; M Weber, 'Bureaucracy', in H Gerth and W Mills (eds), *From Max Weber: Essays in Sociology* (Routledge [1921–1922] 2009)

11 Bok (n 4) 4, 21.

12 J Derrida, 'Archive Fever: A Freudian Impression' (1995) 25(2) Diacritics 9–63, 11, fns 1, 12, 17.

13 Weber (n 10).

Secrecy then is potent but hazardous. Controlling the supply of information enables the secret-holder to influence 'what others know, and thus what they choose to do', meaning secrets also offer power to their holders.[14] Secrecy has a capacity, amplified at group and state level, to produce fanatical, obsessive, conspiratorial behaviour, only curbed by separating the functional benefits of secrecy from the risks contained in its symbolic power and continually balancing it against the imperative of publicity.[15] Of course, secrecy can be productive and useful. The tradition of secrecy in the family courts is protective and secrecy in the form of Chatham House Rules can facilitate discussion not otherwise publicly appropriate.

State secrecy should refer to an institutionally or culturally deliberate concealment which is powerful and dangerous. The existing literature only hints at this but in several competing perspectives; none of which, I contend, adequately captures this idea as a whole. Those that discuss state secrecy directly[16] describe it as an exceptional power and facet of control,[17] an institutional necessity,[18] and a constraint on transparency and accountability.[19] These existing conceptions are: (a) geographically and contextually inappropriate as they are largely concerned only with the USA; (b) insufficiently map on to the reality of state secrecy as an ordinary and standard cultural practice even in liberal democratic states like the UK and the USA; (c) as a consequence of (b), fail to capture that state secrecy seeks to obscure how commonplace it is; and, finally, (d) do not capture that state secrecy has a plurality of modes.

In the twenty-first century, state secrecy has largely been seen as an exceptional form of power or control. It regulates public knowledge and access to information, implying that state secrets are assets, instrumental bolsters to governmental power. Where normal regulation concerns how citizens and corporations behave, state secrecy regulates what they may know.[20] Much of the US literature centres on the so-called 'states secrets privilege' (SSP), a government-wide rather than strictly presidential executive privilege enabling evidence to be excluded from court proceedings.[21] Its power extends far beyond

14 Bok (n 4) 282.

15 Shils (n 6).

16 P Birkinshaw, *Reforming the Secret State* (Open University Press 1990); I Leigh, 'Changing the Rules of the Game: Some Necessary Legal Reforms to United Kingdom Intelligence' (2009) 35(4) Review of International Studies 943–55; A Kelso, 'Response to Bochel et al: "Scrutinising the Secret State"' (2010) 38(3) Policy and Politics 489–90.

17 D P Moynihan, *Secrecy: The American Experience* (Yale University Press 1999); S D Schwinn, 'The State Secrets Privilege in the Post-9/11 Era' (2010) 30(2) Pace Law Review 778; D M Curtin, 'Keeping Government Secrecy Safe: Beyond Whack-A-Mole' Max Weber Lecture Series 07 (European University Institute 2011); D O Thompson and M Garcia, *Veils of Secrecy: Government Practices and Prohibited Disclosures* (Nova 2012).

18 *National Commission on Terrorist Attacks upon the United States* (9/11 Commission Report 2004) 417 <http://avalon.law.yale.edu/sept11/911Report.pdf>.

19 E Goitein and D M Shapiro, *Reducing Overclassification through Accountability* (Brennan Center for Justice 2011); D Cole, 'Confronting the Wizard of Oz: National Security, Expertise and Secrecy' (2012) 44(5) Connecticut Law Review 1617–25, 1624.

20 Moynihan (n 17).

21 R M Pallitto and W G Weaver, *Presidential Secrecy and the Law* (John Hopkins University Press 2007); L K Donohue, 'The Shadow of State Secrets' (2010) (159) University of Pennsylvania Law Review 77; M Fenster, 'The Implausibility of Secrecy' (2014) 65(2) Hastings Law Journal 309–63; S Chesterman, *One Nation Under Surveillance* (Oxford University Press 2011); S Aftergood, 'If in Doubt, Classify' (2008) 37(4) Index on Censorship; Schwinn (n 17) 101–7; L Fisher, *In the Name of National Security: Unchecked Presidential Power and the Reynolds Case* (University Press of Kansas 2006).

actual cases as it is primarily used to circumscribe potential litigation, leading to it being referred to as 'graymail'.[22]

While viewing secrets as assets to be regulated captures the situation in a codified system such as in the USA, it is less applicable to the UK where prerogative is still a spectral reality which resists capture. Further, the regulatory position of the respective intelligence agencies differs. While the UK intelligence agencies were an open secret, known but not officially avowed until 1989, and operating under executive and military authority, the US Central Intelligence Agency and National Security Agency have always operated under the statutory authority of the National Security Act 1947. Indeed, the regulatory context of executive power in the USA is shaped by its codified constitutional structure, whereas in the UK the attempt to restrict executive power shapes the constitutional understanding of accountability.

The commodification of information[23] – and its relationship to the structure and history of the UK relevant to state secrecy – is distinct from that in the USA. The culture of secrecy[24] and deference to political elites is a more acceptable custom in British politics than in the USA,[25] where transparency was entrenched in 1966.[26] US statutory intervention arose from the need to break an executive presumption in favour of secrecy[27] and was regarded as revolutionary, particularly since no executive department or agency or the President supported it.[28] It is limited to federal and executive bodies, and records damaging to national security or other government interests are exempted.[29] The UK did not enact transparency legislation until 2000, although not for want of trying (see below).

Commodification is also seen in the view of state secrecy as an institutional necessity. If we focus on the security context, secrecy is often referred to as necessary and functionally indispensable to governments. National security cannot be protected if governments cannot operate partially (or even largely) in secret. Internal secrecy persists as intelligence agencies resist sharing, upholding a 'need-to-know' information-protection culture.[30] Even the legislative branch in the USA lacks immunity from this proprietorial behaviour as national security is used to withhold information from Congress, making secrecy an inter-branch power battle.[31] But again, the USA as an exemplar of this point is not directly transferable to the UK (at least if popular sentiment prevails and the US

22 Donohue (n 21) 82, 85.

23 W M Arkin and D Priest, *Top Secret America* (Back Bay 2011) 176–82.

24 D Vincent, *The Culture of Secrecy: Britain, 1832–1998* (Oxford University Press 1998).

25 R T McKenzie and A Silver, *Angels in Marble* (Heinemann I968); E A Nordlinger, *The Working Class Tories* (MacGibbon & Kee I967); D Kavanagh, 'The Deferential English: A Comparative Critique' (1971) VI(3) Government and Opposition 333–60.

26 The Freedom of Information Act (FOIA) 5 USC §552 1966 developed a 1946 statute. Amendments were passed in the Government in the Sunshine Act 5 USC §552b 1976 referencing Judge Brandeis' proclamation that 'sunlight is said to be the best disinfectant': L Brandeis, 'What Publicity Can Do' *Harper's Weekly* (New York, 20 December 1913).

27 W Ginsberg, 'The Freedom of Information Act (FOIA): Background, Legislation, and Policy Issues' (Congressional Research Service 7–5700/R41933 2014).

28 S J Archibald, 'The Freedom of Information Act Revisited' (1979) 39 Public Administration Review 311–18.

29 FOIA 1966 (n 26).

30 9/11 Commission Report (n 18); Cole (n 19) 1624.

31 H Kitrosser, 'Supremely Opaque? Accountability, Transparency, and Presidential Supremacy' (2010) 5 St Thomas Journal of Law and Public Policy 62.

Constitution is not seen as ambivalent about strict publicity).[32] If anything, institutional necessity is too weak to explain the 'culture of secrecy' present in UK governance.[33]

Consider how in 2009 Justice Secretary Jack Straw warned that excessive publication of sensitive government information would 'be more likely than not to drive substantive collective discussion or airing of disagreement into informal channels and away from the record'.[34] Add that the UK spies on diplomats and politicians,[35] discourages the press from publishing sensitive information (through the D/DA (defence/defence advisory) notice system) and has a police force which uses secret, often controversial, tactics to monitor protest movements.[36] Finally, place those facts next to Bentham's words who, while espousing that 'without publicity, no good is permanent: under the auspices of publicity, no evil can continue',[37] also argued secrecy is acceptable to protect the innocent, prevent unnecessary punishment or when publicity would favour the projects of an enemy.[38] The result is a perspective which sees secrecy as part and parcel of the standard operating procedure of government, meaning that, where state secrecy is discussed as a necessity, it would be no short leap to recognise and explain secrecy as a normal and normalised mode of governing in liberal democratic states like the UK and the USA. Its existence is explained by reference to the age of principality and fiefdom coupled with its necessity during the ideological global power disputes of the Cold War. But state secrecy is more than a historical leftover or inter-relational need. State secrecy is not alien but *a*, if not *the*, cultural mode of British politics and by extension a key driver of power. It informs government behaviour, is the behavioural premise of security and intelligence service power and the investigatory approaches taken by the police, and grounds the legislative intention of acts which purportedly regulate state surveillance, although in reality likely encourages more of it.

The reality of state secrecy is not reflected in the idea of either power and control or institutional necessity. It is easy to sell state secrecy as a public good in a culture where it has deep roots, but this does not reflect its hazardous potential. However, in many ways the two are polar perspectives. The power-and-control view takes a negative view, whereas the institutional-necessity view casts state secrecy in a positive light, drawing out its essential role in the feasibility of government action. A workable and useful conception of state secrecy would need to combine both perspectives.

32 G Epps, *American Epic* (Oxford University Press 2013); US Constitution, Article 1, s 5, allows for secrecy in congressional proceedings; Pallitto and Weaver (n 21); Foreign Intelligence Surveillance Act 1978 and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (US PATRIOT Act) is also relevant here.

33 Vincent (n 24).

34 HC Deb 24 February 2009, vol 488, col 154.

35 'GCHQ Intercepted Foreign Politicians' Communications at G20 Summits' *The Guardian* (London, 13 June 2013) <www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits>.

36 *R (on the Application of Catt) v Commissioner of Police of the Metropolis* [2015] UKSC 9; the identity of Mark Kennedy, who controversially infiltrated environmental protest groups, was concealed at trial (*R v Theo Bard and Others* [2014] EWCA Crim 463), 'Prosecutors Improperly Withheld Crucial Evidence from Trial of Protesters' *The Guardian* (London, 10 June 2015) <www.theguardian.com/uk-news/undercover-with-paul-lewis-and-rob-evans/2015/jun/10/prosecutors-improperly-withheld-crucial-evidence-from-trial-of-protesters>.

37 J Bentham, 'Of Publicity (Political Tactics)', *The Collected Works of Jeremy Bentham* (Clarendon Press [1843] 1999) 39.

38 Ibid.

Nor can these perspectives account for the kind of state secrecy which is not intended to assert a power, insulate from internal or external criticism, control an agenda, or manage public perception. Clearly, it is powerful and does control public perception, governmental behaviours and agendas, but state secrecy also self-generates (see below) and perceptions of secrecy can invite greater scrutiny and scepticism about government behaviour. Donohue's notion of 'graymail' shows how the SPP is actually used far more widely than the case law suggests; Sagar's account of the role of leaking in politics to control the release of information inadvertently neatly demonstrates how far information is commodified and therefore jealously protected; and Curtin illustrates from an EU perspective the true extent of executive discretion to conceal.[39] Until you go looking for attempts to conceal, it is seen as extraordinary, whereas in fact secrecy and secret-keeping proliferate and always have done so.

The blindness to state secrecy's commonality in the USA is shown in the Brennan Center for Justice's recent report on secret law.[40] It states, somewhat baldly, 'the United States does not have a tradition of secret law'.[41] This statement is curious given that the US Constitution was drafted in secret,[42] and the extent and use of the state secret's privilege and other executive powers. It is true legislation has always been published and 'a commitment to transparency took root early in the nation's history and has for the most part remained strong', *symbolically* speaking.[43] Given the report goes on to outline three *systemic* challenges to the legal pursuit of transparency,[44] it is curious that its authors would begin with a plainly inaccurate claim unless, of course, they do not wish to challenge US political and constitutional mythology by accepting that secrecy is, legally and politically speaking, commonplace. Further, to focus on the idea of 'law' is unhelpfully narrow given most secrecy occurs at a policy level. Nevertheless, this awkward juxtaposition of constitution-founding mythology and reality is informative in the conceptual analysis of state secrecy. When the perspective is flipped from transparency and accountability to an inquiry into the meaning of state secrecy, its persistent and arguably ingrained role becomes apparent. It changes state secrecy from an exception to a norm.[45]

Secrecy's necessity also subtly co-opts debates on the need for governmental transparency and accountability, with even its harshest critics recognising minimal utility in state secrecy.[46] Sagar claims 'there is broad agreement that state secrecy is justified . . . [if] it is used to protect national security and not to conceal wrong doing'.[47] This is accepted despite strong evidence of the damage state secrecy inflicts. In the balance

39 Donohue (n 21); R Sagar, S*ecrets and Leaks: The Dilemma of State Secrecy* (Princeton University Press 2013); D Curtin, 'Judging EU Secrecy' (2012) 2 Cahiers de Droit Européen 459–90.

40 E Goitein, *The New Era of Secret Law* (Brennan Center for Justice, New York University School of Law 2016) <www.brennancenter.org/sites/default/files/publications/The_New_Era_of_Secret_Law_0.pdf>.

41 Ibid 3.

42 Epps (n 32); A Amar, *America's Constitution: A Biography* (Random House 2005).

43 Goitein (n 40) 3.

44 Indeed, it also notes 'the design of the Constitution suggests that some level of secrecy within the executive branch may be tolerated or even protected'; Goitein (n 40) 4.

45 G Agamben, *State of Exception*, K Atwell (trans) (University of Chicago Press 2004); J Ferejohn and P Pasquino, 'The Law of the Exception: A Typology of Emergency Powers' (2004) 2(2) International Journal of Constitutional Law 210; B Honig, *Emergency Politics: Paradox, Law, Democracy* (Princeton University Press 2009).

46 S Aftergood, 'Reducing Government Secrecy: Finding What Works' (2009) 27(2) Yale Law and Policy Review 399–416.

47 Sagar (n 39) 16.

between secrecy and transparency, secrecy often wins.[48] Indeed, there is cognitive dissonance on information rights and transparency. Information released on request does not mean the organisation has been transparent or co-operative. The information was not actively released, or open and ready to be viewed at will; it had to be requested, thus requiring knowledge that the information existed. This difference is what made Edward Snowden's leaks[49] so significant. Both an implementation programme and a willingness to comply are needed for authentic openness.[50] When state secrecy is seen as something to balance against accountability, the focus slips towards *how* to balance it, overlooking state secrecy's subtler effects and outright neglecting the pre-assigned weight given to secret information.[51]

Having identified that existing commentary draws state secrecy in at least three different ways, it might seem unfair to claim there is no recognition of state secrecy existing in plural modes. However, none explicitly discusses the distinct forms or modes, either in their reflection on state secrecy or by surveying across the different scholarship. Without such recognition the conception is narrow, concentrated on security, and more easily justified. The extent of state secrecy in the UK is hard to grasp because it is a patchwork of formal statutory provisions, informal regulatory structures and underlying cultural practices which commodify information and see scrutiny as a danger not a value. Nevertheless, it is precisely this range which requires that even a minimally adequate definition of state secrecy needs to be understood as something which has plural, although related, modes.

2 The architecture of secrecy

Even at its most basic level the pursuit of state secrecy is both more complex and more elusive than might be expected. In the UK, it is not found in one configuration, but is comprised of an overlapping patchwork of formal structures, semi-formal regulatory mechanisms and informal cultures and practices. These are comprised of three elements:

- the formal institutionally secretive structures, such as the security and intelligence agencies, as well as the relevant law enforcement agencies, which while not secretive by design can operate in secret;
- the semi-formal regulatory mechanisms which are used to limit and control access to government material, such as the Official Secrets Act 1911–1989 and various civil actions;
- and, finally, the informal 'need to know' culture which not only characterises the relationship between the government, the people and external agencies but also between departments and units, as well as between the government, Parliament and the courts.

48 Chesterman (n 21); Aftergood (n 21).

49 *The Guardian*, 'NSA Files: Decoded – What the Revelations Mean for You' <www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>.

50 R Hazell, B Worthy and M Glover (eds), *Does Freedom of Information Work? The Impact of FOI on Central Government in the UK* (Palgrave Macmillan 2010).

51 A Ashworth 'Taking a "balanced" view of the public interest' in *The Hamlyn Lectures: Human Rights, Serious Crime and Criminal Procedure* (Sweet & Maxwell 2002); J Waldron, 'Security and Liberty: The Image of Balance' (2003) 11(2) Journal of Political Philosophy 191–210.

This patchwork lays bare not only the long secretive history of British espionage,[52] but the cultural practice of secrecy,[53] a product of the aristocratic attitude to governing in which both Parliament and the public 'abdicate its powers' to the executive to scrutinise secrecy.[54] Citizens must trust those elected and appointed representatives, who represent the 'honour' system of British politics,[55] when their rights are curtailed for generalised and unspecified threats. They must trust a system which initially developed sanctions for breaching government secrecy not to protect the public but to prevent unauthorised disclosure.[56] Even watershed moments seemingly limiting executive power in fact reinforced and formalised it,[57] and, as we shall see, in the post-2001 counter-terrorism context there has been a new age of prerogative matching the structure of risk and security politics.[58]

Secretive institutions, behaviours and 'oversight'

Three institutions and their related committees[59] are especially relevant to state secrecy in the UK: the Security Service (or MI5); the Secret Intelligence Service (SIS) (or MI6); and GCHQ. Until 1989 they were popularly known,[60] but only as a badly kept public secret.[61] Placing these agencies under statutory authority provided the missing dimension, not only of their operation, but of constitutional law.[62] After numerous failed attempts to minimise access to information about MI5,[63] the Security Service Act (SSA) 1989 outlined MI5's powers and authority to defend the realm and maintain national security against espionage, terrorism and sabotage.[64] This extensive power also includes safeguarding the UK's economic wellbeing.[65] As a 'self-tasked' organisation, MI5 assesses its own priorities for action, a measure intended to ensure ministerial restraint and protect the service from accusations of political and partisan action.[66] In reality this advisory role provides a space for MI5 to monopolise its power.

52 T Cowdry, *The Enemy Within: A History of Espionage: Spymasters and Espionage* (Osprey 2006).

53 Vincent (n 24); Crossman (n 2).

54 C M Andrew, *The Defence of the Realm: The Authorized History of MI5* (Allen Lane 2009) 753; *Council of Civil Service Unions (GCHQ) v Minister for the Civil Service* [1985] AC 374, in particular per Lord Diplock at 952.

55 Vincent (n 24) 315.

56 D Hooper, *Official Secrets: The Use and Abuse of the Act* (1987) 17, 21; Major and Moran (n 8) 27–37.

57 FOI 2000 exemptions.

58 T Poole, Poole 'United Kingdom: The Royal Prerogative' (2010) 8(1) International Journal of Constitutional Law 146–55, 154.

59 Joint Intelligence Committee, the Joint Terrorism Analysis Centre and the National Security Committee. Supported by a National Security Advisor and National Security Secretariat, *The Strategic Defence and Security Review: Securing Britain in an Age of Uncertainty* (Cm 7948 2010) §6.1.

60 *Lord Denning's Report into the Profumo Affair* (Cmnd 2152 1963) detailed security services management and published the previously internal 1952 Maxwell Fyfe Directive. They had also been discussed in popular literature and some judicial documents since 1909.

61 Two earlier Acts indicated their existence and provided funding: the Civil List and Secret Service Money Act 1782 (repealed 1977) and the Government of Ireland Act 1920; P Birkinshaw, *Freedom of Information: The Law, the Practice and the Ideal* (Cambridge University Press 2010) 33.

62 Andrew (n 54) 28; Birkinshaw (n 61) 369.

63 Andrew (n 54); S Rimington, *Open Secret: The Autobiography of the Former Director-General of MI5* (Hutchinson 2001); Chesterman (n 21).

64 SSA 1989, s 1(2).

65 Ibid s 1(3).

66 I Leigh, 'Intelligence and the Law in the United Kingdom' in L K Johnson (ed), *The Oxford Handbook of National Security Intelligence* (Oxford University Press 2010) 642.

In contrast, as the furore surrounding the Snowden leaks demonstrates,[67] there is a continued reluctance to be candid about SIS (MI6) and GCHQ despite their recent moves to present themselves as more open (including GCHQ joining Twitter).[68] MI6 supplies the government 'with a global covert capability to promote and defend' national security and the economic well-being of the UK.[69] GCHQ, the eavesdropping agency, monitors radio and satellite transmissions in overseas countries and is the largest intelligence agency, with a staff of over five thousand.[70] In the 1980s, MI6 and GCHQ were the subject of public controversy,[71] but they were only officially acknowledged in 1992 and confirmed in the Intelligence Services Act (ISA) 1994. The statutory provisions are deliberately opaque,[72] outlining the astonishingly wide function to obtain and provide information on actions or intentions of persons outside the British Islands and other related tasks.[73] GCHQ obtains, monitors and 'interferes' with electromagnetic, acoustic and other emissions and any equipment producing such emissions.[74] These institutions sit at the forefront of the conception of state secrecy because common sense suggests that intelligence-gathering and spying relates directly to secrecy and much of the secretive behaviour of the state is undertaken to serve intelligence and surveillance functions.

All three agencies are also governed by another set of contentious legal provisions, which provide powers to other public bodies to operate and investigate in secret. Until 2016, investigatory powers were governed under the labyrinthine Regulation of Investigatory Powers Act (RIPA) 2000 and Data Protection and Investigatory Powers Act (DRIPA) 2014, which have been replaced with the already heavily criticised and judicially contested[75] Investigatory Powers Act (IPA) 2016. As the Explanatory Notes to IPA 2016 acknowledge, the powers provided largely already existed, including the interception of communications, the retention and acquisition of communications data, equipment interference, and the acquisition of bulk data. However, the IPA 2016 extends those powers and officially acknowledges others. But as DRIPA 2014 has been found inconsistent with the privacy protections in the EU Charter of Fundamental Rights in *Watson*,[76] and the IPA 2016 is substantially modelled on those provisions, it seems it will be open to challenge (the Court of Appeal is yet to rule on the extent of the

67 Z Bauman et al, 'After Snowden: Rethinking the Impact of Surveillance' (2014) 8(2) International Political Sociology 141–44.

68 GCHQ, '"Hello, World"': GCHQ Has Officially Joined Twitter' (16 May 2016); 'The Web Is a Terrorist's Command-and-Control Network of Choice' *Financial Times* (London, 3 November 2014) <www.gchq.gov.uk/news-article/hello-world-gchq-has-officially-joined-twitter>; <www.ft.com/content/c89b6c58–6342–11e4–8a63–00144feabdc0#axzz3I7Jjs7jf>.

69 ISA 1994.

70 MI5 employs around 4000 people <www.mi5.gov.uk/who-we-are> information is not available for SIS/MI6staff numbers.

71 *GCHQ* (n 54); and highlighted by the *Spycatcher* saga, see below.

72 L Lustgarten and I Leigh, *In from the Cold: National Security and Parliamentary Democracy* (Clarendon Press 1994) 65.

73 ISA 1994, s 1(1).

74 Ibid s 3(1).

75 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen* (C-203/15) and *SS for the Home Department v Tom Watson et al* (C-698/15) ECLI:EU:C:2016:970 [2016].

76 Ibid.

inconsistency). The issue will remain even after Brexit as *Watson* draws directly on European Court of Human Rights (ECtHR) language.[77]

In relation to state secrecy, the act does four things. One, it introduces new powers in the guise of matching technological change. The fallout from the Snowden revelations and suggested need to plug 'capability gaps'[78] provided an opportunity to surreptitiously broaden surveillance powers to allow collection of bulk datasets,[79] the deployment of 'thematic' warrants[80] and in Parts 3 and 4 extend power to gather and retain communications data. For example, it placed government hacking, known as equipment interference (EI), on a statutory footing, thereby legitimising its use.[81] Two, it strengthens existing surveillance powers. In addition to the 'targeted interception' powers which allow access to the content of communications,[82] Part 2 also provides measures to enable 'thematic warrants', allowing groups of individuals to be targeted[83] where they share 'a common purpose or . . . carry on, or may carry on, a particular activity'.[84] No definition or limit is given on what size or type of group can be targeted. Were the powers to acquire information not strong enough, the Act also enables highly intrusive bulk personal data sets (BDPs) in Part 7 which capture data from 'a wide range of individuals, the majority of whom are unlikely to be of intelligence interest'.[85]

Three, it places an onus on private services providers to hold data for the government in case it is needed for national security. The Act co-opts the data-gathering activities of tech companies through technical capability notices (TCNs) and national security notices (NSNs).[86] With an NSN, a minister can require telecoms companies to take specified measures with respect to national security and TCNs require such companies to maintain the ability to remove encryption (even if this is not practically possible).[87] Finally, the Act also claims to improve the oversight system by consolidating existing oversight bodies into a new Investigatory Powers Commissioner[88] and providing the 'double-lock' mechanism whereby both the relevant minister and a commissioner approve warrants

77 *Zakharov v Russia* [GC] ECtHR 2015 47143/06 [119]; A Patrick, 'Who Sees You When You're Sleeping? Who Knows When You're Awake?' UK Human Rights Blog (21 December 2016) <https://ukhumanrightsblog.com/2016/12/21/who-sees-you-when-youre-sleeping-who-knows-when-youre-awake>.

78 D Lyon, 'Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique' (2014) 1(2) Big Data and Society 1–13.

79 IPA 2016, Parts 6 and 7.

80 Ibid Part 2, s 17.

81 Ibid Part 5.

82 Ibid Part 2, s 20(2)(c) and s 20(4).

83 Part 2, s 17.

84 Part 2, s 17(2)(a).

85 Intelligence and Security Committee of Parliament, 'Privacy and Security: A Modern and Transparent Legal Framework' (HC 1075 2015).

86 IPA 2016, s 252.

87 See 'Could the UK Be about to Break End-to-end Encryption?' TechCrunch (27 May 2017) <https://techcrunch.com/2017/05/27/could-the-uk-be-about-to-break-end-to-end-encryption>; 'UK Government Can Force Encryption Removal, but Fears Losing, Experts Say' *The Guardian* (London, 29 March 2017) <www.theguardian.com/technology/2017/mar/29/uk-government-encryption-whatsapp-investigatory-powers-act>.

88 IPA 2016, Part 8, s 227.

before they become effectual.[89] Significantly, in urgent circumstances this approval can be *ex post facto*.[90]

What does this mean for state secrecy? Commentary has long focused on intrusive surveillance and data-gathering in terms of privacy and due process rights.[91] The tendency is to ask who authorises access to data and meta-data – until recently an overlooked aspect of data collection.[92] It is hard to dispute that a thwarted terror attack is better than a successful one, but prevention should not be a carte blanche. There is little debate about legitimacy or necessity of secrecy in intelligence and security, or at least debate that is not motivated by external factors such as the ECtHR.[93] The assumption seems to be that extensive secretive powers operate on the assumption of political and legal trust without testing the foundation or architecture of that trust.[94] Just as RIPA 2000 did before it, IPA 2016 conceals that key provisions are vaguely worded and structurally tangled, and rely on blunt assertions of executive privilege regarding national security which, along with serious crime,[95] remains undefined in statute and is so broadly applied it is considered meaningless.[96]

The statutory provisions for investigatory powers hint at the scope of secrecy because they demonstrate that the state wants to collect information on its own citizens as well as foreign nations (and nationals) and how it will go about doing so. The powers indicated for a large range of bodies governed by and encapsulated by the IPA 2016 and earlier provisions are far-reaching. The possibility of effective oversight of those powers has similarly been captured by the cloaking demand of secrecy. For instance, the scrutiny of the security and intelligence agencies has been at best haphazard and at worst deliberately complicated. Prior to statutory provision, oversight took the same form as any other prerogative power. The agencies' directors general and chiefs deliver internal oversight providing annual reports to the Prime Minister.[97] External oversight evolved after a patchy start (the Security Service Tribunal did not uphold a single complaint in its first three years)[98] into a more cohesive framework under RIPA 2000.[99]

89 IPA 2016, Part 2, s 19 and s 23.

90 Ibid s 24.

91 K Ewing, *Bonfire of the Liberties* (Oxford University Press 2010).

92 L K Donohue, 'Bulk Metadata Collection: Statutory and Constitutional Considerations' (2014) Georgetown Law Faculty Publications 1350.

93 Curtin (n 17).

94 D Anderson, Independent Review of Terrorism Legislation, *A Question Of Trust: Report of the Investigatory Powers Review* (OGL 2015) <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf>.

95 Serious crime is left undefined: G Robertson, 'Recent Reform of Intelligence in the UK: Democratization or Risk Management?' (1998) 13(2) Intelligence and National Security 144–58, 148.

96 D Korff et al, 'Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes' (2017) Global Report <https://ssrn.com/abstract=2894490>.

97 SSA 1989, s 2, and ISA 1994, s 2(2) both with relevant amendments in the Security Service Act 1996; Leigh (n 66).

98 M Phythian, 'The British Experience with Intelligence Accountability' (2007) 22:1 Intelligence and National Security 75–99, 77.

99 IPA 2016, s 234. The Investigatory Powers Commissioner replaces the Intelligence Services Commissioner which covered MI5 and MI6, and the Interception of Communication Commissioner which covers GCHQ (RIPA 2000, Part IV, ss 57–64).

The Investigatory Powers Tribunal (IPT), which hears complaints about communication interceptions and any security and intelligence matters, has been criticised for providing only nominal accountability.[100] Until 2015, when the IPT finally dared to find any agency behaviour unlawful[101] (albeit this behaviour now complies), there were no 'publicly recorded examples of a tribunal finding against any of the services'.[102] Accountability efficacy depends on various factors, including agency willingness, but between 2001 and 2007 *none* of the 600 complaints was upheld, and to 2011 a mere 10 of 1301 complaints were upheld.[103] Moreover, the 2011 and 2015 statistics in the IPT's report excludes all 660 complaints relating to Privacy International's 2015 campaign.[104] The annual report is further tainted by secrecy as it is subject to redaction 'if it appears . . . contrary to the public interest' or any other functions of the services.[105] While, as *Watson* indicates, conformity to necessity and proportionality standards will continue to circle the Act, a recent case suggests the limits to judicial review for investigatory powers are further tightening.[106]

Ineffectual parliamentary scrutiny further bolsters this secrecy. The Intelligence and Security Committee (ISC) introduced in 1994 was intended to bolster external oversight, but lacked teeth and so was replaced by the Intelligence and Security Committee of Parliament,[107] which is still not particularly effective. The Prime Minister can exclude any prejudicial information from its annual report[108] and delay its publication, significantly curtailing parliamentary debate. While reports have been more forthcoming in recent years, greater scrutiny is achieved in large part due to the committee members' expertise and 'ability to divine' the right questions.[109] The committee is further restricted by its domestic remit, the need for prime ministerial permission to scrutinise operational activities and the Cabinet's ability to veto demands for agency material. Since only one committee is trusted (officially and unofficially) to oversee the security and intelligence agencies, parliamentary oversight is remarkably inhibited.[110]

Information control

Information is controlled through three intersecting mechanisms: measures which ostensibly provide, but in fact restrict, access to information (FOI 2000 exemptions and the ministerial veto); criminal sanctions (the Official Secrets Act 1911–1989) and civil actions (confidence, third-party liability and contract).

100 Leigh (n 16) 648.

101 *Prism/Upstream case: Liberty and Others v FCO (the Security Service, SIS, GCHQ)* [2015] UKIPTrib 13_77-H.

102 Leigh (n 16) 648.

103 Ibid 648.

104 Report of the Investigatory Powers Tribunal 2011–2015 (OGL 2016) <http://ipt-uk.com/docs/IPT_Report_2011_15.pdf>.

105 IPA 2016, s 234(2), para 651; previously RIPA 2000, s 58(7).

106 *Privacy International v IPT* [2017] EWCA Civ 1868.

107 Justice and Security Act (JSA) 2013.

108 JSA 2013, s 3(4); Birkinshaw (n 16) 49.

109 M Phythian, 'A Very British Institution: The Intelligence and Security Committee and Intelligence Accountability in the United Kingdom' in L K Johnson (ed) (n 66) 715.

110 A Defty, 'Recent Events at the Intelligence and Security Committee', Democratic Audit UK (30 May 2015) <www.democraticaudit.com/?p=5706>; H Bochel, A Defty and A Dunn, 'Scrutinising the Secret State: Parliamentary Oversight of the Intelligence and Security Agencies' (2010) 38(3) Policy and Politics 483–7.

The UK came late to a statutory right to access public information[111] and only after significant retreat from the original proposals.[112] Official information was something to control not share. Earlier provisions such as the Public Records Acts 1958–1967 detailed a 30-year rule after which public records could be released,[113] unless the documents were still in use or of particular sensitivity.[114] Material relating to national security and defence could be closed for longer. The FOI 2000 sought to engender a vital change from the prevalent need-to-know culture to presumption in favour of disclosure.[115] Most agree these expectations were not met.[116]

Despite being applicable to any body performing a public function, outlining a positive duty to provide information, or at least confirm its existence,[117] and imposing a response time limit,[118] there are 23 exemptions to the application of FOI 2000 falling into two main categories: qualified (class and harm-based)[119] and absolute. Qualified exemptions are subject to a public interest balancing test,[120] although the Act 'fails conspicuously to say anything at all'[121] on the definition of public interest. The nine absolute exemptions prohibit discretionary public interest disclosure covering information relating to security, court records and parliamentary information prejudicing effective conduct of public affairs.[122] Public authorities need not confirm or deny the requested information's existence.[123] National security is also covered by the harm-based exemption and is defined by ministerial certificate (applicable to any of the 17 qualified exemptions), catching anything not covered by the Official Secrets Act 1989 and the Security and Intelligence Acts (1989, 1994, 1996). Although ministerial certificates can be challenged by the Information Commissioner and the First-Tier Tribunal (Information Rights), in some cases the certificate itself counts as conclusive evidence of the exemption being in the public interest.[124] Ministers can also veto disclosure on

111 FOI 2000; by way of comparison, Sweden enacted legal provision in 1776, USA 1966, Canada 1982, New Zealand 1982 and Australia 1982.

112 HC Deb 28 July 1999, vol 570.

113 The Public Record Office and the National Archives at Kew.

114 Public Records Acts 1958–1967, s 3(4).

115 Home Office (Freedom of Information Unit), *Your Right to Know: Freedom of Information* (Cm 3818 1997).

116 Birkinshaw (n 61) 118–19; C Hood 'From FOI World to Wikileaks World: A New Chapter in the Transparency Story?' (2011) 24(4) Governance: An International Journal of Policy, Administration, and Institutions 635–38, 637.

117 FOI 2000, s 1.

118 Ibid s 17(1)(c).

119 Class-based information can be withheld regardless of harm; harm-based exemptions are subject to a prejudice test (FOI 2000, s 2 and Part II); see further Home Office (n 115) 3.7.

120 Guidance is provided by the Information Commissioner, the 2004 Code of Practice on Access to Government <http://webarchive.nationalarchives.gov.uk/20150603223450/https://www.justice.gov.uk/downloads/information-access-rights/foi/foi-section45-code-of-practice.pdf.>.

121 M Turle, 'Freedom of Information and the public interest test' (2007) 23(2) Computer Law and Security Report 167–76, 167.

122 FOI 2000, ss 23, 32 and 36 respectively.

123 Ibid Part 1, s 2(1)(b).

124 Ibid s 2(2)(b), ss 23 and 24 in particular.

'reasonable grounds'.[125] The recent battle to prevent the release of the 'Black Spider Memos' shows this has been used politically, as much as for true public interest.[126]

It is worth noting how much this contrasts with the seeming advance of transparency in general. The FOI 2000 has provided a straightforward way to request information. Indeed, it has irritated the very politicians that enabled it with both politicians and mandarins complaining about the impositions the Act created. For example, Tony Blair expressed his 'regret' at the introduction of the FOI 2000 as it 'hugely constrained' ministers' confidence in having frank discussions with advisors.[127] Of course, this frustration is not relevant to the exemptions nor is it clear what kind and extent of transparency is produced by some FOI requests.[128] The UK might be beginning to follow the ECtHR trend to view the FOI 2000 as a general duty to provide information without needing to first request it, but again this is a matter as much of politics as it is of law and requires understanding the other mechanisms available to limit the flow of information.[129]

Information is also controlled by the informal Government Protective Marking Scheme (GPMS), which provides four classification levels – top secret, secret, confidential and restricted.[130] These bear no relation to the Official Secrets Act 1911–1989 sanctions but may be adduced as evidence of likely harm or damage in court.[131] These markings impart a practice valuing secrecy over transparency and are further complicated by D or DA notices, a voluntary press self-censorship system.[132] The controversial system,[133] which depends largely on media acquiescence, has been significantly undermined by the internet age, but its continued existence is indicative of the governmental preference for closed processes.

This all needs to be seen in the context of the formal criminal sanctions relating to state secrecy in the Official Secrets Act 1911–1989.[134] The Act's brevity disguises its power.[135] It outlaws espionage, sabotage and unauthorised and damaging disclosures of official information. The 1989 incarnation replaced the excessively blunt[136] if not

125 Ibid s 53; Hazell et al (n 50) 356.

126 *R (Evans) v Attorney General* [2015] UKSC 21; see M Elliot's analysis, 'Of Black Spiders and Constitutional Bedrock: The Supreme Court's Judgment in Evans' Public Law for Everyone (26 March 2015) <https://publiclawforeveryone.com/2015/03/26/of-black-spiders-and-constitutional-bedrock-the-supreme-courts-judgment-in-evans>; Craig (n 1).

127 T Blair, *A Journey* (Random House, 2010) 516; Public Administration Committee, Oral Evidence (HC 1582-iv, 23 November 2011).

128 M Fenster, 'The Opacity of Transparency' (2006) 91 Iowa Law Review 885–949; A Colquhoun, 'The Cost of Freedom of Information' (Constitution Unit, University College London, December 2010) 2 <www.ucl.ac.uk/constitution-unit/research/foi/countries/cost-of-foi.pdf>.

129 *Magyar Helsinki Bizottság v Hungary* (2016) ECHR App 18030/11 <http://hudoc.echr.coe.int/eng?i=001–167828>.

130 Home Office (Franks Committee), *Report on Section 2 of the Official Secrets Act 1911* (Cmnd 5104 1972) §62.

131 Birkinshaw (n 16) 92.

132 <www.dnotice.org.uk/danotices/index.htm>

133 Major and Moran (n 8) 155; N Wilkinson, *Secrecy and the Media: The Official History of the United Kingdom's D-notice System* (Routledge 2009); Hooper (n 56) 224, 226.

134 Official Secrets Act 1911–1989 is currently the subject of a Law Commission consultation seeking to recommend reform, including stricter punitive measures and removing 'barriers' to prosecution like the damage test: *Protection of Official Data: A Consultation Paper* (Law Com No 230, 2017) <www.lawcom.gov.uk/wp-content/uploads/2017/02/cp230_protection_of_official_data.pdf>.

135 Prior to 1989, the Act was more instrumental as a threat than a sanction (Franks Committee (n 131) §13:123), and the pedestrian pace of reform could be read as deliberate.

136 Birkinshaw (n 16) 367.

draconian s 2 in its entirety.[137] Section 1 offences are subject to a reverse burden defence,[138] placing the onus on the alleged person to prove they did not know or reasonably believe the information would be damaging.[139] Quite how a person could prove this is another matter; presumably security and intelligence personnel and notified persons have little room for manoeuvre in this respect. However, in a substantial departure from the 1911 Act, mere receipt of information by a third party is no longer an offence. And yet, while ordinary citizens are the least restricted, they are in fact the most in the dark, unlikely to ever be privy to the most 'sensitive' information. Further, there is no settled consensus on the authorisation procedure, leaving room for political manoeuvring around unauthorised disclosure.

While the use of civil actions has waned in recent years, they nevertheless play a key role in information control alongside criminal sanctions. The law of confidence has been used to maintain cabinet secrecy (*Crossman Attorney General v Jonathan Cape Ltd* [1976] QB 752); to cover third-party liability (*Spycatcher*); and restitutionary damages have been sought for breach of contract (*Attorney General v Blake* [2001] AC 268). The now infamous *Crossman* diaries case, saw Jonathan Cape Ltd and the *Sunday Times* sued for breach of confidence on the basis of Cabinet responsibility, in particular relying on the privy counsellor's oath, presumably as secrecy associated with collective Cabinet responsibility is ignored when it suits the government. The case was not an outright win for either side; any confidence owed was held to have passed,[140] and confidence is a matter of circumstance not rule.[141]

The *Spycatcher* saga, much too convoluted to warrant detail here,[142] is a farcical episode in the history of state secrecy and shows the absurd lengths the state will go in order to maintain control. At the centre of the litigation is whether a breach of confidence (either in equity or contract)[143] could extend to other jurisdictions, third-party liability for that breach and the extent of the public interest in disclosure or non-disclosure of information.[144] To the government's chagrin, Wright, a former British spy, sought to

137 Franks Committee (n 131) §88:37; Hooper (n 56) 123; Birkinshaw (n 16); and the occasional historic cases (*R v Tisdall* [1985] (Unreported, 23 March 1984), the failed prosecution of Clive Ponting (*R v Ponting* [1985] Crim LR 318) and the Aitken trial (*R v Aitken* (Unreported 1971); J Aitken, *Officially Secret* (Weidenfeld & Nicolson 1971) 22, 56, for a sense of the history.

138 The *mens rea* requirement was significant in reform, see *Reform of Section 2 of the Official Secrets Act 1911* (Cmnd 7285, 1978) §7:7; Aitken (n 138) 22, 56; Birkinshaw (n 16) 3.

139 Official Secrets Act 1989, s 1(5).

140 Per Widgery at 771.

141 H Young, *The Crossman Affair* (Hamish Hamilton 1976) 203; the subsequent Radcliffe Report maintained a preference for common law approach, but recommended formalising the vetting and approval system for proposed publications, including a 15-year rule publication bar: Select Committee on Public Administration (Radcliffe Report), *Report of the Committee of Privy Counsellors on Ministerial Memoirs* (Cmnd 6386, 1976) §45–57, 83–6.

142 There were multiple concurrent parts to the five-year litigation: an Australian case (*Attorney General for the UK v Heinemann Publishers Australia Pty Ltd* (1987) 8 NSWLR 341; *Attorney General for the UK v Heinemann Publishers Australia Pty Ltd* (1987) 10 NSWLR 86 and *Attorney General for the UK v Heinemann Publishers Australia Pty Ltd (No 2)* (1988) 78 ALR 449); an appeal to the interlocutory Millet injunctions (*Attorney General v Guardian Newspapers Ltd (No 1)* [1987] 3 All ER 316 – hereafter *Spycatcher (No 1)*); a hearing on the permanent injunctions (*Attorney General v Guardian Newspapers Ltd (and Others) (No 2)* [1990] 1 AC 109 – hereafter *Spycatcher (No 2)*); contempt of court proceedings (*Attorney General v Newspaper Publishing plc* [1987] 3 All ER 276) and ECHR Art 10 cases (*Observer v UK* (1992) 14 EHRR 153; *Times Newspapers Ltd and Neil v UK* (1993) 15 EHRR CD49).

143 *Spycatcher (No 2)*.

144 The clash of rival philosophies per Scott J, *Spycatcher (No 2)*, 143.

disrupt myths about the propriety and importance of shielding the UK's security and intelligence regime from public view. As injunctions have only domestic force, the court found itself the arbiters of a case already decided by the ensuing tumult in the international press.[145]

Despite the cat irrefutably being out of the bag, several principles emerged from the ruling: when using confidence to suppress official information, harm to the public interest must be proven; third-party disclosure in breach of confidence has a limited defence of iniquity; and public interest cannot necessarily be sustained once the information has already been disclosed.[146] The potential harm and indeed contact with national security, from the 'exceptionally dull book itself'[147] following worldwide publication, had 'become rather remote'.[148] Indeed, quite far from showing irreparable damage, the government admitted several claims were already published in '12 books and three television programmes'.[149] But this did not stop the government at the ECtHR[150] bizarrely claiming *Spycatcher* focused on national security when the substantive discussion was on confidentiality's limits.[151] This blurring of the line between public and private law, dubiously implying necessity, is a pattern repeated in *Blake*,[152] which also demonstrates how state secrecy is shaped by a Cold War mentality. The case's paradigmatic language highlights how an incendiary approach is a tactic in state secrecy cases:[153] Blake was a traitor, a double agent. Alleged treachery and risk to national security is a 'knock-down' argument, requiring no further discussion.

Post-2001 counter-terror context

Much of the legal framework for state secrecy, formal and informal, was formed in an earlier era, but has now been embedded in a post-2001 counter-terrorism context. State secrecy mechanisms have mushroomed since 2001: there have been at least 10 legislative attempts to increase the power of the government to protect national security and limit access to information.[154] This high volume demonstrates how controversial and problematic these acts and amendments are. Changes were often the result of growing judicial intervention.[155] Successive governments have been Janus-faced, promoting democracy while eschewing transparency and legitimacy as priorities. It is only on the basis of significant Acts like the Human Rights Act 1998 and the FOI 2000 that limited

145 *Spycatcher (No 2)*, 156.

146 *Spycatcher (No 2)*, 222. This arises again in *Attorney General v Punch* [2002] UKHL 50, which effectively closed a potential law of contempt loop-hole opened by the Court of Appeal's ruling: see R Earle, and N Hanbidge, 'Temporary Injunctions: Punch and the Paper Tiger' (2003) 14(3) Entertainment Law Review 62–3.

147 Ewing (n 91) 143.

148 Per Lord Bingham, *Spycather (No 2)*, 224.

149 *Observer v UK* (1992) 14 EHRR 153, 220.

150 *Times Newspapers Ltd and Neil v UK* (n 143); *Observer v UK* (n 143).

151 Per Morenilla *Observer v UK* (n 143) 219.

152 *Attorney General v Blake* [2001] AC 268.

153 A W B Simpson, 'A Decision per Incuriam?' (2009) 125 Law Quarterly Review 433.

154 Terrorism Act 2000, Anti-Terror, Crime and Security Act 2001, Criminal Justice Act 2003, Prevention of Terrorism Act 2005, Terrorism Act 2006, Counter-Terrorism Act 2008, Terrorism Prevention and Investigation Measures Act 2011, Justice and Security Act 2013, Crime Justice and Courts Act 2015 and Counter-terrorism and Security Act 2015.

155 *A and Others v Secretary of State for the Home Department* [2004] UKHL 56 (*Belmarsh*); *Secretary of State for the Home Department v Rehman (AP)* [2001] UKHL 47; R *(Binyam Mohamed) v Secretary of State for Foreign and Commonwealth Affairs* [2010] EWCA Civ 158, EWHC Civ 65 (*Binyam Mohammed and BM); Secretary of State for the Home Department v JJ and Others* [2007] UKHL 45; *Secretary of State for the Home Department v MB*; *Same v AF* [2007] HL; *Gillian and Quinton v UK* [2010] ECHR 4158/05.

restrictions were available, but, where possible, even these were subverted. Public interest immunity (PII) certificates and closed material procedures (CMP) have crept into more areas to protect government information and MI5, MI6 and GCHQ agents. This includes expanded use of government-vetted special advocates[156] to inhibit the courts' ability to scrutinise questionable government behaviour and subvert the rule of law.[157] Similarly, the use of terrorism prevention and investigation measures (TPIMs), the successor to control orders, enables individuals to be restricted in a number of ways, utilising civil sanctions as anticipatory measures at a lower standard of proof.[158]

These measures are usually discussed in the language of emergency and necessity to protect national security.[159] The Explanatory Notes to the recent Counter-terrorism and Security Act 2015 describe the 'heightened threat to our national security'.[160] In many ways, emergency has ceased to represent the exceptional and become the norm. It allows the standard and expected aspects of the law to be replaced by a norm of emergency where 'the state of exception appears as the legal form of what cannot have legal form'.[161] But in the UK these powers are *residual* powers that have been replaced in the constitutionalising (and liberalising) efforts of the twentieth century: in order to recreate them, they must be recreated in legal form. The UK has become a fortress state, where state secrecy is the norm and where information is kept from the external actors as well as internal.

3 Conceptualising state secrecy

What does this legal and political patchwork tell us about the concept of state secrecy? The concept must encapsulate the extent of its power and its ability to commodify information, as well as its tendency to conceal itself and creep into a wide range of government practices. The following section outlines three *overlapping* parts to the concept which could be considered models of state secrecy. Some aspects of secrecy fit within more than one category at a time, but appear different cast in the alterative light. As all secrecy involves intentional concealment, the three concepts are distinguished in part by intentionality. Consider who intends to conceal, what is intended to be concealed, and from what public.

Esoteric secrecy

The first concept identified is esoteric state secrecy,[162] referencing the etymological and philosophical meaning, not the common understanding of abstruse or incomprehensible. Arising from the Greek *esoterikos*, from *esotero*, meaning 'inner', esoteric refers in this stricter sense to that designated or intended for an inner or privileged group. Insiders are

156 J Ip, 'Al Rawi, Tariq, and the Future of Closed Material Procedures and Special Advocates' (2012) 75(4) Modern Law Review 606–23; C Murphy, 'Counter-terrorism and the Culture of Legality: The Case of Special Advocates' (2013) 24(1) King's Law Journal 19–37, 37.

157 A Hunt, 'From Control Orders to TPIMs: Variations on a Number of Themes in British Legal Responses to Terrorism' (2014) 62(3) Crime, Law and Social Change 290, 296; A Kavanagh, 'Special Advocates, Control Orders and the Right to a Fair Trial' (2010) 73(5) Modern Law Review 836–57.

158 A Ashworth and L Zedner, *Preventive Justice* (Oxford University Press 2014).

159 M Tushnet, 'Emergency Law as Administrative Law' in F Davis and F de Londras (eds), *Critical Debates on Counter-terrorism Judicial Review* (Cambridge University Press 2014) 121; C Gearty, 'State Surveillance in the Age of Security' in F Davis, N McGarrity and G Williams (eds), *Surveillance, Counter-terrorism and Comparative Constitutionalism* (Routledge 2014).

160 Counter-terrorism and Security Act 2015.

161 Agamben (n 45) 1.

162 Referencing Curtin (n 17) 7, but used differently.

privy to the secret. Outsiders are persons to whom the secrets are not revealed. It is a privilege to be deemed to have the expertise to be initiated as an insider. The content is less important than *who* controls the information and makes it secret.

Esoteric state secrecy limits the number of persons with a specific range of expertise who can be responsible for ensuring safe continuity of the nation, in other words, national security, covering anything from physical safety; the maintenance of borders; the detection and prevention of any threats; economic and stabilising factors such as the maintenance of a functioning economic market producing adequate wealth; to trade and bargaining power on an international platform. For example, national security is a founding premise of the Official Secrets Act 1911–1989 which criminalises espionage and the unlawful disclosure of information and protects state secrets. Only those who fall within a particular category or status are authorised to see and handle classified information. They are 'initiated' by 'signing' an Official Secrets Act declaration, a non-legally binding document making them aware of their obligations under the Act. Those transgressors who break rank and publicise information relating to national security without authorisation face retributive measures. The information might reveal the identity of insiders or reveal the knowledge insiders are privy to. Esoteric secrecy calls on parts of the state to be deferential to those within the sphere of power. The executive defers to its national security advisors, in other words, to its experts.

Esoteric state secrecy is stratifying. It creates groups of persons, an elite to whom particular (and powerful) information is available. Simply being part of the traditional 'elite' (the judiciary, the upper chamber of Parliament, the wealthy, the aristocratic and the corporate highflyer) does not admit one to the esoteric arena of state secrecy. This is a particular governmental and political privilege. Not all MPs or government ministers are cognisant of information concerning national security. The heads of the security and intelligence agencies report only to the Prime Minister and the relevant Secretary of State.[163] This institutes a principle of exclusion on the basis of expertise. If you are not the Commander-in-Chief (or de facto the commander's vested executive authority, such as the Prime Minister), or the government or Cabinet, or a person responsible for national security, you are neither able to determine the content of national security nor examine the evidence the determination is based on. Anyone not deemed an expert by those within will not be privy to national security information. Whether the Prime Minister and Cabinet members are experts, as a matter of fact, is a further question. For the exclusion claim, however, it is sufficient to accept they are since this is the current practice. This exclusion subverts the principles on which the ability of those who hold power is premised. The coterie has the expertise to represent and determine the public interest. The public 'consent' to government power, but only if there are measures to limit that power; but with government power, the position of privilege, the public cannot but accept the claim that those in power know more, know better. An expert is harder to challenge. Esoteric state secrecy provides an answer to the question 'Who gets to decide?' in the case of national security by curtailing the debate from the political and public realm and placing it only in the reach of 'those who need to know'.

Operational secrecy

The second conception, operational secrecy, is demonstrated by focusing on the UK's secret institutions. If for esoteric secrecy the relevant aspect of intentional concealment was *who* controlled information, operational secrecy is concerned with *why* they control

163 SSA 1989, s 2(2); ISA 1994, s 2(2).

information and *which* information they control. It is a functional argument, referencing the information's content. MI5, MI6 and GCHQ have never been very secret but have always been secretive. The secrecy is an imperfect arrangement accepted because absolute secrecy is neither achievable nor politically desirable. Stories of MI5, of British spies, of royal spies, of their exploits and achievements have abounded since their inception, if not before. Which begs the question, what is secret about MI5, GCHQ and MI6 if they are the worst kept secret in history? The answer is they were never intended to be secret in this sense. The concealment of their existence was a consequence of the covert manner in which they operate; their existence was never intended to be secret. The manner in which they behave is one characterised as 'hush-hush'. Reference is made to 'sources', 'advising' and 'intel'. Mention of the institutions and organisations from which information arises, at least prior to the twenty-first century, was scant.

The security and intelligence services' secrecy is the product of omission. The secrecy of their existence is pretence. It is no pretence, however, that their activities, procedures and tactics are most definitely secret. The domestic service was 'acknowledged'[164] as early as 1910 in an informal sense, but official avowal[165] provides a poor point of reference for operational procedure and technique. Details of current operations and procedures within the security and intelligence agencies is sparse or entirely absent. Whether or not the security and intelligence agencies successfully maintain control over operational secrecy is a separate question. They cannot control discussion and speculation about their activities.[166] This inability to prevent speculation references the idea of deep and shallow secrecy,[167] outlined below. Information the public knows exists but cannot access is shallow and information the public does not even know exists is deep. The security and intelligence agencies are shallow secrets, although some of their operations are deep secrets.

MI5, GCHQ and MI6, while not strictly secret or a deep secret, nevertheless typify operational secrecy in the UK. Their concern is to protect modern espionage techniques or 'tradecraft', as the intelligence terminology calls it.[168] This safeguards their procedures and techniques and conceals their activities and investigations from their targets. Operational secrecy refers to fragile and time-limited information, as well as information which has a longer 'shelf-life' or technical usage. There is still value in protecting knowledge of techniques used, even if a particular operational result is made public. There is a separate, more philosophical discussion here about the difference between theoretical and practical knowledge. Oakeshott criticised the rationalist preference for theoretical over practical knowledge.[169] But for the purposes of understanding the concept of operational secrecy, it suffices to say operational secrecy values both theoretical and practical knowledge. The work of the security and intelligence services is as much about preventing those engaged in espionage, sabotage, subversion and terrorism from acquiring a theoretical knowledge of the practices of MI5, MI6 and GCHQ as it as it is about surveillance of such persons.

164 Andrew (n 54) 28.

165 SSA 1989 and ISA 1994.

166 Fenster (n 129).

167 D Pozen, 'Deep Secrecy' (2010) 62 Stanford Law Review 257–339, 258.

168 L K Johnson (ed) (n 66) 14, 60.

169 M Oakeshott, 'Rationalism in Politics' in *Rationalism in Politics and Other Essays* (Liberty Fund [1962]/2nd edn 1991) 15.

The regulation of the security service, MI5, exemplifies operational secrecy. It is 'self-tasked', assessing its own priorities for action. The government provides some guidance on policy and the Intelligence and Security Committee performs oversight. With a domestic service, ministerial restraint is required, otherwise the Home Secretary or the Cabinet could be accused of requiring the service to act in a political or partisan manner.[170] But maintaining this 'arms-length' approach to policy provides room for a different kind of political controversy. MI5 justifies its autonomous advisory role on the basis of its expertise. Its self-tasked mandate, which keeps covert action outside domestic politics, is premised on prior advantages. The security services, observed Lord Neuberger, 'have an interest in the suppression of information'.[171] MI5 has an interest in maintaining the highest level of operational secrecy achievable because it reduces the scope for scrutiny of its work.

The statutory provisions reveal the extent to which this operational secrecy pervades the relationship between the agencies and government. While the directors general of MI5 and MI6 and the chief of the intelligence service (GCHQ) must produce an annual report for the Prime Minister and the Home or Foreign Office Secretary, there is no obligation for the Prime Minister to lay this report before Parliament or even the Intelligence and Security Committee.[172]

The Intelligence and Security Committee itself has offered the bare minimum penetration into the working procedures of the security and intelligence services until very recently. It was not a traditional Select Committee, with its attendant powers, but a 'committee of parliamentarians', executively appointed in consultation with the leader of the opposition. The Security and Justice Act 2013 rectified this, but the committee still suffers internal barriers to effective oversight. The publication of its annual report is invariably delayed to such a point when its contents are no longer of political interest. It can be redacted by the Prime Minister where the information is deemed to be 'prejudicial to the continued discharge of the functions of the services'.[173] In its 2015/2016 report there are 31 instances of redaction, most of which appear to relate to the budget in the appendices to an otherwise distinctly short report (five pages of actual text).[174] The 2013/2014 report only contains two-and-a-half pages of substantive text, one section of which relates to the death of a previous committee member.[175] The 2011/2012 report has 51 instances of redaction of uncertain length and detail.[176] A great deal of effort is expended on diluting the already weak powers of oversight over the security and intelligence services. Greater scrutiny is achieved at present only through the skills and expertise applied by those members of the committee divining the right questions to discover the underground well of security and intelligence behaviour.

Oversight is largely internal. The introduction of a single IPT under RIPA 2000 did little to change the nominal status of the complaints system. Between 2001 and 2007 there were 'no publicly recorded examples of a tribunal finding against any of the

170 Lustgarten and Leigh (n 72) 508.

171 The conclusion of the original and final edited 'paragraph 168', per Lord Neuberger MR, *Binyam Mohamed (Civ)* (n 156) 168.

172 SSA 1989, s 2(4), and ISA 1994, ss 2(4) and 4(4).

173 Security and Intelligence Act 2013, s 3(4).

174 Intelligence and Security Committee, *Annual Report 2015–2016* (HC 444 2016).

175 Intelligence and Security Committee, *Annual Report 2013–2014* (HC 794 2014).

176 Intelligence and Security Committee, *Annual Report 2011–2012* (Cm 8403 2011/2012).

services'.[177] Between 2001 and 2011 only 10 of 1301 had sufficient grounds to be upheld.[178] The year 2015 saw ground-breaking finds against the services, but the law had already been adjusted to legalise the practices.[179] Of course, it is possible the security and intelligence services consistently act in a manner beyond reproach, but the more likely explanation is that the system of oversight holds loss of operational secrecy a greater risk. All of which adds up to a great mass of behaviour which simply cannot be viewed through the magnifying glass of oversight and which cannot hope to capture the activities of the security and intelligence services, which by dint of their profession actively seek to act furtively. Their operational capacity can only be viewed through a tiny glass, darkly.

Efficient secrecy

The third concept of state secrecy is efficient secrecy. The state needs some secrecy to function well. Government in most forms operates to some purpose, be it public good, peace, order, the will of an autocrat, maximisation of freedom, or some other such driving factor. It is partly a logical proposition, whatever the purpose, that government should act so as to guarantee that purpose is satisfied.

Esoteric secrecy focuses on who gets to make decisions regarding information control. Operational secrecy focuses on the information's content and the behaviours of secret institutions. Efficient secrecy refers to a different type of information and a different type of public. Rather than information withheld on the basis of an enemy public or a public within, it is withheld from the mandated public (members of the state). It is a partly pragmatic and partly conceptual argument. Both elements refer to the idea of publicity as an ideal in liberal states. Complete publicity, the argument runs, is neither pragmatic nor conceptually possible. It makes no sense to publicise all information, even if you could publicise all information. In terms of an archetype example, efficient secrecy effectively presents two counter-publicity arguments. The first, the pragmatic argument, looks at Cabinet secrecy and the second, conceptual, looks at the limits of transparency.

It is a well-founded idea, arising from public choice theory, that efficient government is better government regardless of the particular political standpoint sought. The drive towards efficiency[180] has been shown to challenge some of the other principles which drive government. For instance, Newey defends political lying. While *prima facie* wrong, lying's wrongness 'is conditional on its violating the autonomy of its (intended) victim'.[181] In a democratic system the professional success of a politician depends on their appeal to the electorate, which is often based on 'highly implausible or blankly false claims about what can be delivered in office'.[182] The electorate recognise the exaggeration or plain falseness, but it still forms the mandate on which the successful politician is elected.

Fenster criticises the claim that transparent government is more efficient. He argues:

> [C]omplete transparency not only would create prohibitive logistical problems and expenditures . . . but more importantly, it would impede many of the

177 Leigh (n 16) 648.

178 Ibid.

179 *Liberty v Security Service, SIS and GCHQ* [2015] UKIPTrib 13_77-H.

180 J M Buchanan, 'Politics, Policy, and the Pigovian Margin' (1962) 29 Economica 17–28; A Breton, 'Toward a Presumption of Efficiency in Politics' (1993) 77(1) Public Choice 53–65.

181 G Newey, 'Political Lying: A Defense' (1997) 11(2) Public Affairs Quarterly 93–116, 106.

182 Ibid 107.

> government's most important operations and infringe upon the privacy interests of individuals who give personal information to the government.[183]

Newey and Fenster, in opting for pragmatism about transparency, claim not only that it is unobtainable but potentially undesirable. It is from these boundaries between competing political ideals that efficient secrecy arises.

Two elements demand consideration in connection with Cabinet secrecy. First, some secrecy in government makes for better, more efficient government because secrecy produces better deliberation and has a hand in producing an executive working in at least a pretence of consensus. Second, Cabinet secrecy is as much about the way in which the public is 'prepared' for the release of information. The Franks Report outlined the Cabinet need to retain the ability to discuss issues 'frankly and fully in private'.[184] The basis of Cabinet secrecy is the doctrine of collective responsibility. Were Cabinet discussions not secret, collective unity and the integrity of the discussions of the Cabinet would be damaged.[185] This goes further than the argument justifying secret discussions concerning national security. It potentially insulates the decision-making process within the Cabinet from scrutiny, or at least manages the way scrutiny is applied.

The *Crossman* diaries litigation is the classic statement of the protection of Cabinet secrecy. The issue in *Crossman* was whether the significant detail had yet passed into 'historical interest only'.[186] The antiquated practice at the basis of Cabinet secrecy imparts a duty of confidentiality. The Cabinet developed from a committee of the Privy Council, the formal body of advisors to the monarch. The Cabinet was once a committee which advised rather than decided. The procedure is inversed today, the Cabinet decides on behalf of the monarch and advises the monarch who (nominally) assents. As an advisory body, the Cabinet owed a duty of confidence to the monarch, underscored by the privy counsellor's oath. Members of the Cabinet are de facto privy counsellors and are required to take the oath, a duty of secrecy regarding matters discussed in Cabinet. The oath signifies the confidence privy counsellors owe as the sovereign's advisors, ensuring the Cabinet acts as one body and its parts owe a duty of confidentiality to the whole.

The decision in *Crossman* demonstrates the second factor in efficient secrecy, the idea of timing and presentation. While it was held that confidentiality and public interest exist with respect to the Cabinet, both were deemed time limited. The most common break with the principle of Cabinet secrecy is the regularity of leaks prior to announcements, which emphasises how timing is relevant to the idea of efficient secrecy. Widgery J claimed leaking 'is an accepted exercise in public relations'.[187] Information management, in this sense, is a strategic interpretation of Cabinet secrecy. Adjusting Bacon's aphorism, control of knowledge is power. Cabinet secrecy maintains that government works better when it controls when and how information is released. A well-timed leak can assist the government in preparing the public for a controversial decision in the same way a delay in publicising a decision can wait out the storm of conventional politics. These tactics are not necessarily a political or public good but attempt to secure efficient government. A controversial but necessary decision might fare better if government does not have to defend it in the court of public opinion.

183 Fenster (n 129) 902.

184 Franks Committee (n 131) §11:66.

185 Ibid §11:68.

186 *Crossman* at 759 §D.

187 Ibid 770, §E.

Secrecy in the service of the state has its origins not in the hard-won constitutional privileges or even the tacit assent on the part of the ruled populace, but in the very practice of rule. At its most basic, it ensures the survival of the state.[188] Efficient secrecy through the archetype of cabinet secrecy highlights a tension at the heart of liberal political theory.

On the one hand, political discourse is better when it is held in public, publicly available and open to as many people as possible. Political discourse denotes political decision-making, both the decisions made and the manner in which those conclusions are reached. According to Bentham, this universality suggests the inescapable viability of publicity as the 'fittest law for securing the public confidence'.[189] Only through publicity can the electorate act from knowledge. Secrecy, argues Bentham, is 'an instrument of conspiracy; it ought not, therefore, to be the system of a regular government';[190] whereas publicity exposes politics to the cleansing light of scrutiny. As Brandeis famously has it, sunlight is the best disinfectant.[191] Bentham gives three exceptions to the rule of publicity which are too narrow and idealistic to be of help. The 'fittest law' is to be suspended when its effects 'favour the projects of an enemy', unnecessarily injure innocent persons, and inflict too severe a punishment on the guilty.[192] Bentham gives little explanation for what he means by each of these. The meaning in the first two is relatively clear, but the third is less so.

On the other hand, efficient secrecy directly challenges Bentham's conception by suggesting secrecy has a role to play *even* when the general rule of liberal politics conforms to publicity. Decision-making and the process of deliberation leading to decisions can often be more efficiently and effectively made in closed spaces, by a limited number of persons. O'Neill notes '[a] well known result of debate is further debate, rather than the ending of all disputes'.[193] Publicity here is invoked in clear contradiction to most claims for publicity. Secrecy enhances deliberation. Removed from the pressures and brightness of complete publicity, debate is more reasonable, more flexible and results ultimately in more rational public outcomes.[194] Secrecy can benefit high-level discussions because members can 'speak candidly, change their positions, and accept compromises without constantly worrying about what the public and the press might say'.[195]

In addition to its impracticality, absolute publicity is not conceptually feasible. Lessig asks whether the trumpeting of transparency-as-value fails to consider it in a critical manner.[196] While freedom of information does not mean absolute transparency, the crippling, debilitating effects of too much transparency, with its consumption of energy and resources, could make for an inert political system. If we return to efficient government as one which acts towards some purpose, to champion a system which would paralyse decision-making seems a little perverse. Of course, no one is arguing for complete, absolute transparency. But expansive transparency can create problems. How

188 Pallitto and Weaver (n 21) 93.

189 Bentham (n 37) 29.

190 Ibid 39.

191 Brandeis (n 26).

192 Bentham (n 37) 39.

193 O O'Neill, *Constructions of Reason: Explorations of Kant's Practical Philosophy* (Cambridge University Press 1989) 537.

194 C Chambers, 'Autonomy and Equality in Cultural Perspective' (2004) 5(3) Feminist Theory 329–32, 329.

195 A Gutmann, and D Thompson, *Democracy and Disagreement* (Harvard University Press 1996) 115.

196 L Lessig, 'Against Transparency' *The New Republic* (9 October 2009) <www.newrepublic.com/article/books-and-arts/against-transparency>.

much transparency is enough to oil the wheels of the political machine, motivating government and public alike, and how much would paralyse and produce disaffection? This is a logical sense in which government can and should hold on to some information. It should be less concerned with actively publicising information. The difference is found in the motivating factor, like the difference between an advertent and inadvertent omission, which is key to understanding efficient secrecy.

The concept of transparency 'relies upon an inappropriate model of information and communication to produce an inaccurate understanding of government information'.[197] This is no less true of the concept of secrecy. Without an appropriate model of information and communication, the same tired comprehensions of secrecy will be rehearsed. What is government information? What is communication? Fenster reorients the discussion of information theory to accommodate the understandings arising from hermeneutic and structuralist theories of textual information.[198] The concept of state secrets cannot be based on the assumption that the state is an omniscient singular body, nor can it assume it is internally coherent with respect to the information it does hold. It is a pointless exercise to ask whether freedom of information legislation increases transparency if the model of information control is inaccurate.

Fenster's criticism of transparency is pertinent to the secrecy-for-efficient claim. The traditional account of transparency, presumes the existence of a coherent, responsible and responsive state in the traditional form that exists as a model of democratic government in liberal political theory.[199] Theories of transparency do not pay enough attention to the fractional nature of government. Does the Home Secretary, let alone the civil servants, really know what is going on? Who is doing what in the Foreign Office, in the Cabinet Office, in the Treasury? This is not to claim that there is no communication or collaboration between government departments. Rather it is to suggest epistemologically that anyone's understanding of the government is limited, even those on the inside and in the know.

What does this mean for state secrecy and the concept of efficient secrecy? It suggests, simply, that one person's intentional concealment is another person's unknown. The difficulty – perhaps the impossibility – is in telling the difference. The concept of efficient secrecy contains a potentially irresolvable ambiguity, in much the same way as there is an underlying question at the basis of the freedom of information debate: with whom does the final determination lie? Who ultimately gets to determine what is in the public interest to keep secret, or even, who gets to determine the public interest: the government or the people?

Conclusion

State secrecy is not a monist concept. It is supported by complex institutional, legislative, political and cultural structures and practices. This exploration of the concept of state secrecy has produced a tripartite definition. State secrecy is esoteric, operational and efficient. Esoteric describes the part of state secrecy that restricts access to decision-making and information. It is a facet of power, utilised to control. Operational describes state secrecy-protecting techniques, procedures and investigations. It is not as all-encompassing as esoteric secrecy but can accumulate through the employment of jigsaw theory. Finally, efficient secrecy describes state secrecy as functional and the product of

197 Fenster (n 129) 949.

198 Ibid 925.

199 Ibid 915.

the limits of transparency. Functional decisions are made faster and more effectively under secret conditions. The limits of transparency make secrecy inevitable as well as useful. The tripartite conceptualisation encompasses those transferable aspects of the existing literature on state secrecy. Power and control is seen in esoteric and operational secrecy. Institutional necessity is seen in operational and efficient secrecy. Efficient secrecy better describes how state secrecy is necessary but in need of balance and provides the boundaries of how that balancing might take place. The tripartite conceptions also make sense of the relationship between the three conceptions by giving content to the idea of state secrecy as in flux.

What does this tripartite definition of state secrecy tell us? State secrecy suppresses its own history, hiding its ingrained role in political history and the security rhetoric of the early twenty-first century. State secrecy as esoteric, operational and efficient provides public law with a perspective from which to explore not just the impact on civil liberties, but how and why state secrecy is a risky but fundamental part of the UK's constitution. By understanding what state secrecy is, as a legal entity and a socio-political behaviour, better regulatory practice can be established, challenging the security and intelligence agencies to work with and within scrutiny. It challenges the repetitive unsubstantiated claim of necessity, ensuring that, if it must exist, it is an intentional, not incidental, state secrecy, thereby bringing state secrecy to the democratic approach the UK purports to uphold, one which is vigilant to the dark charm of secrecy.