Max Weber Lecture Series

MWP – LS 2011/07
MAX WEBER PROGRAMME

KEEPING GOVERNMENT SECRECY SAFE:
BEYOND WHACK-A-MOLE

Deirdre M. Curtin

EUROPEAN UNIVERSITY INSTITUTE, FLORENCE

MAX WEBER PROGRAMME

Keeping Government Secrecy Safe: Beyond Whack-a-Mole

DEIRDRE M. CURTIN

MAX WEBER LECTURE No. 2011/07

ISSN 1830-7736

Printed in Italy
European University Institute
Badia Fiesolana
I – 50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu
cadmus.eui.eu

Abstract

The concept of secrecy as a mechanism for not providing government information, on the one hand, and the commitment to openness of government, on the other, reflect certain historical understandings of the relationship between a government, citizens, officials and information. Within democratic systems of government secrecy has been an essential ingredient irrespective of the existence or otherwise of a written Constitution (eg. US and the UK). The transparency 'explosion' of recent decades both in rhetoric and in law has been matched by a parallel growth in secrecy regulation and practice at all levels of government, including, in Europe, supranational government (the EU). Leaking has always had a symbiotic relationship with secrecy. What has changed in the information age is that (leaked) information can be shared right across the globe through the Internet in an unstoppable fashion (Wikileaks).

This lecture focuses on the understudied phenomenon of government secrecy, its nature, structure, categories and its multiple layers. These are explored from the perspective of (representative) democracy and of constitutional law. The basic argument is that secrets can be protected more effectively and more legitimately if government secrecy is reduced overall and more checks and balances introduced.

Keywords

Secrecy, openness, leaking, national security, administrative rationale, European Union, internal security, checks and balances.

The lecture was delivered on Wednesday 16 March 2011

Deirdre M. Curtin
University of Amsterdam

Beyond Wikileaks

The ancient myth of *Pandora's box* is just one of the many tales of calamities befalling those who uncover what is concealed, who release dangerous forces that should better have been left in darkness and silence. The recent opening of Pandora's box by Wikileaks brought, according to some, possible calamity to the US government, and international relations more generally, because of the unauthorized disclosure of classified military secrets.

The leaker within the US government – a rogue junior information analyst with a Top Secret clearance, working in the middle of the Iraqi desert, Private Bradley Manning – is in prison under harsh conditions and awaits trial on charges that could keep him in jail for 52 years, according to the Army.[1]

Reactions to the intermediary Wikileaks, personified in Julian Assange, range from wanting him drawn and quartered for his act of high treason[2] to those who see him as a modern day republican hero worthy of a Nobel Peace Prize nomination.[3]

The criminal laws that penalize the unauthorized release of classified information in principle only apply to government officials like Manning although there are some provisions of the Espionage Act from 1917,[4] adopted to counteract *spying* shortly after the US entered the First World War, that might apply more broadly to those who gather, transmit or 'lose' classified defence information.[5] Its provisions have been interpreted to cover the activities of foreign nationals overseas, at least when they take an active part in seeking out such unauthorized classified information.[6] The US Supreme Court has stated, however, that the question remains open whether the publication of unlawfully obtained information by the media can be punished consistent with the First Amendment of the US Constitution.[7]

The so-called "*Shield Act*"which stands for *Securing Human Intelligence and Enforcing Lawful Dissemination* was introduced in both Houses of the US Congress in 2010. Its purpose is to amend the US Espionage Act (1917) so as to be able to criminally prosecute those who *publish* such leaked information or facilitate its publication. Its scope of application will be applicable to non-US residents acting overseas.[8] This is a typical knee-jerk reaction by an executive power to leaking: an attempt to shore up secrecy even more. If adopted many argue that it could have huge implications for constitutional fundamental rights and freedoms.[9] It is ironic that it is introduced during a Presidency that was launched with open government as one of its *leitmotifs*[10] and with a clear presumption in

---

[1] Bradley Manning may even face the death penalty according to some, see further, <www.guardian.co.uk/world/2011/mar/03/bradley-manning-may-face-death-penalty>.

[2] See further, <www.cbsnews.com/8301-503544_162-20024903-503544.html>.

[3] Julian Assange, founder of the website Wikileaks, has in fact been nominated for a Nobel Peace Prize, see further, <rt.com/politics/assange-nominated-nobel-prize/>.

[4] Act of October 6, 1917, ch. 106, § 10(i), 40 Stat. 422. See also, 18 U.S.C. § 952 (prohibiting the disclosure or publication of certain diplomatic material obtained "by virtue of ... employment by the United States").

[5] See further, the analysis by J. Elsea, "Criminal Prohibitions on the Publication of Classified Defense Information". Available at: <www.fas.org/sgp/crs/secrecy/R41404.pdf>.

[6] See further, for details and limitations, J. Elzea, *ibid*. at p. 26.

[7] The First Amendment to the U.S. Constitution provides: "Congress shall make no law ... abridging the freedom of speech, or of the press...". See further, J. Elzea, *ibid*, at p. 17.

[8] See further, testimony given in a Hearing before the Committee on the Judiciary House of Representatives, 6 December 2010, *Espionage Act and the Legal and Constitutional Issues Raised by Wikileaks*. Available at: <judiciary.house.gov/hearings/printers/111th/111-160_63081.PDF>.

[9] See further, testimony, 6 December 2010, *ibid*.

[10] See, memorandum for the Heads of Executive Departments and Agencies on "Transparency and Open Government" issued by the White House on President Obama's first day in office. Available at: <www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment/>.

favour of openness not secrecy[11]. One of the paradoxes of Obama's Presidency is that he at the same time seeks to broaden and deepen the reach of secrecy regulation and actively prosecutes leakers.[12]

Leaking has always had a symbiotic relationship with secrecy and is the classic way of outing possible abuse of power. [13]

Without secrecy there would be no need to leak information. As government secrecy grows and comes to involve more people, the opportunities to leak from within expand. An organisation like Wikileaks relies primarily on *user generated content*, namely leakers. The novelty lies both in the *amount* of information digitally made available (the total is 251,287 documents downloaded onto a number of usb sticks) in a *geographically unrestricted* manner as well as the potential for what can be termed *analytical transparency*.[14] A form of analytical transparency was put into practice with the strategy of linking up with four classical news organizations, *Le Monde*, *El Pais*, *The Guardian* (shared with the NY *Times*) and *Der Spiegel*. Wikileaks can in this context be understood as an example of a new way of challenging government power in the information age by getting previously hidden information with possible evidence of abuse of power out into the open in a largely unstoppable and global fashion.[15]

In this lecture I highlight the manner in which such government secrecy has expanded dramatically since 9/11 both in the US and in Europe and its various facets. In so doing I argue in favour of taking the need for government secrecy seriously but in order to do so propose we narrow down what genuinely needs to be protected. Only in this way can we ensure that there is a fighting chance that government secrets are indeed kept safe in the modern day world. Moreover we need to introduce more balance with the principles of open government and the citizen's public interest in disclosure, and more checks and balances at least on the content of secrecy rules as such. My core message applies both in the US and in other nation states but also in the context of the supranational *European Union* where there is an urgent need to reconsider the layering of secrecy rules and practices.

Secrecy conceptualised

The sociology of secrecy

But first let me dwell on the conceptual question: what does secrecy mean? Scholars have struggled with the general concept of secrecy for centuries. Sociologists have stressed for more than a century that it is the act of secret keeping that makes us who we are: our inside is not something we have but something we make, partially through our secrets[16]. Or as Harvard philosopher Sissela Bok put it: "Some capacity for keeping secrets and for choosing when to reveal them, and some access to the underlying experience of secrecy and depth, are indispensable for an enduring sense of identity, for the

[11] See, memorandum for the Heads of Executive Departments and Agencies on freedom of information act issued by the White House. Available at:

<www.whitehouse.gov/the_press_office/FreedomofInformationAct/>.

[12] In just over two years since President Obama took office, prosecutors have filed criminal charges in *five* separate cases involving unauthorized distribution of classified national security information to the media. This is more than all other Presidencies taken together (totaling three). No criminal charges have as yet been filed against Julian Assange.

[13] See, S. Bok, *Secrets: On the Ethics of Concealment and Revelation* (Pantheon Books: New York, 1982), at p. 217.

[14] On analytical transparency see further, T.D. Davenport, *Process Innovation: Reengineering Work through Information Technology* (Harvard Business School Press, Boston, 1993).

[15] See further, the two books that have been published on the collaboration with the New York Times, *Open Secrets: WikiLeaks, War and American Diplomacy*. Available at: <www.nytimes.com/opensecrets/>. And the Guardian journalists, D. Leigh and L. Harding, *Wikileaks – Inside Julian Assange's War on Secrecy*, (Guardian Books, 2011).

[16] See in particular, G. Simmel, "The Sociology of Secrecy and of Secret Societies", *The American Journal of Sociology*, 11(4), 1906, pp. 441-498.

ability to plan and to act, and for essential belonging. With no control over secrecy and openness, human beings could not remain either sane or free."[17]

Anything can in fact be kept secret – a path, a plan, a decision – so long as it is kept intentionally hidden, *set apart in the mind of its keeper* as requiring concealment.[18] It may be shared with no one *or* confided to some on condition that it goes no farther. In the words of Bok again: "To keep a secret from someone, then, is to block information about it or evidence of it from reaching that person, and to do so intentionally… The word "secrecy" refers to the resulting concealment."[19] It also covers the *methods* used to conceal, such as codes or disguises or camouflage, and the *practices* of concealment, such as trade secrecy or professional confidentiality.[20]

Secrecy presupposes *separation*, a setting apart of the secret from the non-secret, and of keepers of a secret from the excluded targets. It establishes insiders and outsiders, groups of "us" and "them". Control over secrecy and openness gives *power*: it influences what others know and thus what they choose to do.[21] As Simmel put it already in 1906: "Secrecy is a universal sociological form, which, as such, has nothing to do with the moral valuations of its contents. On the one hand secrecy may embrace the highest values. On the other hand, secrecy is not in immediate interdependence with evil, but evil with secrecy".[22] In other words, wrongdoing, illegality, unethical behaviour will in all likelihood be hidden from public gaze. The reason for 'outing' secrecy and subjecting it to controls is precisely because of this link.

The esoteric and national security rationale for public secrecy

Moving from the personal to the public, Simmel argues that secret keeping actually endows secrets with *value*.[23] This value is based not on the content of the secrets but rather on the fact that others are excluded from knowing about them. The act of secrecy "gives the person enshrouded by it an exceptional position".[24] This is something that human beings seem to know instinctively. A common children's boast is: "I know something you don't".

Such behaviour is not limited to children. Like children, kings were aware that they could maintain special status by *possessing* not exclusive property, but *exclusive information.* The ancient principle of *arcana imperii : the "mysteries of state"* transferred the aura of sacredness from the *arcane ecclesiae* of church and religious officials to secular leaders and was never more strongly invoked than in defence of seventeenth-century absolutist monarchies. Through the doctrine of the *divine rights* of monarchs, secret government was given sanctity of its own.[25]

Kings and governments may however *abuse* their subjects and citizens with the power they gained through the possession of information, and they can use secrecy to cover up any wrongdoing. *Secret government* has for this reason been under challenge for at least a century across the world. "Secrecy is an instrument of conspiracy," wrote Jeremy Bentham, "it ought not, therefore, to be the system of a regular government".[26] Woodrow Wilson spoke out firmly against secrecy in his 1912 election campaign, concluding, "Government ought to be all outside and no inside".[27] Yet once elected to the US presidency he fell far short of imposing the ideal of complete openness that he had

---

[17] S. Bok (1982), *op. cit.*, at p. 24.

[18] *Ibid*, at p. 5.

[19] *Ibid*, at pp. 5-6.

[20] *Ibid*, at p. 6.

[21] *Ibid*, at p. 282.

[22] G. Simmel (1906), *op. cit.*, at p. 463.

[23] *Ibid*, at p. 464.

[24] *Ibid*, at p. 464.

[25] See further, S. Bok (1982), *op. cit.*, at p. 172.

[26] J. Bentham, *The Works of Jeremy Bentham*, published under the Superintendence of his Executor J. Bowring (Edinburgh: William Tait, 1838-1843), Vol. 2. Chapter: *CHAPTER II.: OF PUBLICITY*, para. 4.

[27] See, T.W. Wilson, *The New Freedom*, Leipzig, 1913, p. 113.

advocated.[28] It was in fact during his Presidency that the Espionage Act was adopted and applied in a manner highly restrictive of free speech.

As John Jay wrote in *The Federalist* the executive might sometimes need "perfect secrecy and immediate dispatch".[29] Traditionally, some amount of secrecy is considered valuable for concealing plans and vulnerabilities from adversaries, acting quickly and decisively against threats, protecting sources and methods of intelligence gathering and investigating the law and enforcing it against offenders.[30] A similar line of argument is used to support secrecy in international negotiations and in diplomacy more generally.

But even where no outside enemies or spies threaten and even where appeals to the esoteric rationale for secrecy have dwindled, a degree of secrecy is needed by government in order to be able to function effectively and also in order to protect state secrets and national security.[31] *National security* is the key justification traditionally given for classifying documents as confidential, secret and top secret. It is an important concern that may justify firm limits on governmental openness. National security (or foreign policy) often has an explicit *target* in the sense of a party against whom the government is taking action. Publicising information about these policies poses a special risk of ruining the underlying objective.[32]

The problem lies in the fact that there is a widespread tendency to regard national security as *a trump card*, which leads to an unwillingness to establish credible checks and balances in the adoption of the rules.[33] For example, the US Freedom of Information Act sets as its first exemption matters withheld for national security reasons under criteria established by executive order and "properly classified according to an executive order".[34] This gives the executive power a virtually unlimited discretion (executive prerogative) to withhold information from the public domain.

There is however another rationale for maintaining government secrecy beyond that of national security, international negotiations and diplomacy and it can be referred to as the administrative rationale for secrecy.

The scope of the administrative rationale

The administrative rationale for control over secrecy extrapolates from the individual's claims to such control in order to protect plans in the making, their implementation and confidential relationships.[35] Max Weber already commented on the inherent nature of bureaucracies to be secret. "Every bureaucracy seeks to increase the superiority of the professionally informed by keeping their knowledge and intentions secret".[36] Concealment in fact insulates administrators from criticism and interference; it allows them to correct mistakes and to reverse direction without costly, often embarrassing explanations; and it permits then to cut corners with no questions being asked.

A key argument in this regard is that rationality and efficiency are served by a measure of secrecy in administration. As the British *Francks Committee* wrote in 1972 ministers and administrators must, in order to present clear issues to the Parliament and to the electorate, be able in

---

[28] S. Bok, *op. cit.*, at p. 171.

[29] J. Jay, "The Powers of the Senate", *Federalist Paper No 64*, 7 March 1788.

[30] See, D. Pozen, "Deep Secrecy", *Stanford Law Review*, 62(2), 2010, pp. 257-339 at p.277.

[31] See, S. Bok, *op. cit.*, p. 175.

[32] See, D.Pozen, op.cit. at p.275.

[33] See, A. Roberts, "National Security and Open Government", *Georgetown Public Policy Review*, 9(2), 2004, pp. 69-86.

[34] Executive Order 12356, issued by President Reagan, requires agency records to be classified if their disclosure "reasonably could be expected to cause damage to the national security". Such records, if "in fact properly classified" according to the substantive and procedural rules of the Executive Order, are exempt from mandatory disclosure under the Freedom of Information Act. Available at: <www.nist.gov/director/foia/#ex1>.

[35] S. Bok, *op. cit.*, at p. 175.

[36] See, M. Weber, 'Bureaucracy' in H.H.Gerth and C.Wright Mills (eds.) *Essays in Sociology*. Oxford: Oxford University Press, 1946.

some instances and at some stages to "argue out all the possibilities with complete frankness and free from the temptation to strike public attitudes".[37]

We can refer to this as the *space to deliberate* for ministers and civil servants. The argument is that the existence of this secretive space will lead to the enhanced quality of deliberations and decision-making. If this 'private' space exists then policy makers are said to have more freedom to consider and debate different options, to take risks, to change their minds, to rely on experts. *Privacy* in this sense enables government actors to protect their own domain from unwanted access by outsiders. The need for some 'privacy' protection in the "staging processes"[38] of policy formulation is understandable; the problem is when this secretive space extends way beyond the very initial stages of policy making into the *legislative* process.

The tendency for administrative secrecy to spread is one of the main reasons why *freedom of information laws* are adopted in the first place and attempt a shift towards a presumption of openness as opposed to secrecy.[39] Such laws do not do away with administrative or government secrecy but they do provide access to documents or information in some cases that would otherwise have remained out of reach. Moreover they give statutory and judicial support to the principle of openness. Yet it is striking how governments can on the one hand claim to vigorously pursue open government through freedom of information laws and other measures, yet on the other hand equally vigorously pursue policies and practices of *secret government.* This is to some extent possible because freedom of information laws have on the whole been drafted to accommodate the previously existing secrecy rules on classified information in one form or another.

An example where the administrative rationale has extended way beyond a confined internal space of policy deliberation is the European Union legislative process. Although it has not been explicitly framed in these terms, the European Union has gone quite far down the road of recognizing what some consider as a type of right to informational privacy for government actors[40] in two respects. First, it seems to be accepted that the need for a type of internal space to deliberate applies not only during the early and internal stages of policy formulation by an administration as such but also, and more controversially, during the early stages of *legislative decision-making.* The legislative decision-making process in the EU involves both the European Parliament and the governmental Council of Ministers. They "negotiate" behind closed doors in what are called early first reading 'trialogue' meetings and maintain secrecy over both meetings and documents on the basis of an analogy with diplomatic negotiations, even though the result in over 80% of legislative files is the content of a legislative act.[41] Second, it has been recognised that a government actor such as the European Commission may keep secret the names of those who attend meetings, implying a general right to privacy for those performing public tasks (*Bavarian Lager* case).[42]

The tension between layers of government secrecy and the right of citizens, as expressed in freedom of information legislation, to obtain access to documents or information, can also be expressed in more structural terms. The layers of government secrets extend from what are termed

---

[37] Home Office, *Departmental Committee on Section 2 of the Official Secrets Act 1911*, Cmnd. 5104, September 1972, para. 11.

[38] See, A. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), at p. 45

[39] See, for example, memorandum from 2009 on the Freedom of Information Act (hereafter: FOIA) for the Heads of Executive Departments and Agencies on freedom of information act issued by the White House. Available at:

<www.whitehouse.gov/the_press_office/FreedomofInformationAct/>.

It is expressly stated that "in the face of doubt, openness prevails… all agencies should adopt a presumption in favour of disclosure, in order to renew their commitment to the principles embodied in FOIA, and to usher in a new era of open Government. The presumption of disclosure should be applied to all decisions involving FOIA."

[40] See, in general on this right, A. Murray, "Should States have a Right to Informational Privacy?" in A. Murray and M. Klang (eds.), *Human Rights in the Digital Age* (London: The Glasshouse Press, 2004), at pp. 191-202.

[41] See further on the scope of this phenomenon and for further references, D. Curtin, "The European Parliament and EU Democracy: A Paradox", *Ars Aequi*, November 2009, pp. 708 – 710.

[42] See further my annotation of this case, D. Curtin, "Privacy of EU government data", *Ars Aequi*, March 2011, pp. 20-25.

deep secrets to what are known as *shallow* secrets.[43] Every act of government secrecy can according to David Pozen be located in a continuum between the two poles of deep secrecy and shallow secrecy with the depth of a secret being suggestive of the keeper's intentions. Relative to shallow secret keepers, deep secret keepers will generally be more concerned to conceal from the target the fact that they wish to conceal something. [44]Deep secrets may thus more often involve bad faith or fraud.[45] The targets cannot protect themselves against information they cannot imagine and so the secret-keeper can always gain advantage at the expense of the target.

From deep to shallow secrets

We can best understand the concepts of deep and shallow secrets with metaphors of light. Whereas the deep secret's target is "completely in the dark, never imagining that relevant information might be had" the shallow secret's target "has at least some shadowy sense" that she is lacking relevant information.[46]

When members of the general public understand that they are being denied particular items of information, the result is a *shallow secret*. Both the EU examples of early stage secret legislative procedures and secret government policy meetings are 'shallow' secrets in the sense that their existence is known and knowable, if not their precise content. Freedom of information laws can help outsiders to force more light into the activities and private spaces of insiders. They may or may not be successful in this regard but at the very least the existence of the facts are 'knowable'.

A more problematic category are those 'secrets' that are unknown and thus unknowable via freedom of information legislation or otherwise. When a small group of similarly situated officials conceals from outsiders the fact that it is concealing something the result is a *deep secret*.[47]

Donald Rumsfeld as Secretary of State for defense had this to say on the structure of secrets:

> As we know there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also *unknown unknowns* – the ones we don't know we don't know. And if we look throughout the history of our country and other free countries, it is the latter category that tends to be the difficult ones.[48]

Almost from its moment of utterance – in 2002 – commentators ridiculed Rumsfeld for his "kabbalistic logic and professorial cant". The British Plain English Campaign called it "the most nonsensical remark made by a public figure" in memory.[49]

Yet as David Pozen argues it contains a valid insight that the secrets or things we do not know we do not know are the most difficult ones for a free society. The deeper the secret the fewer the people who will know the secret.[50] But there may also be movement between the categories. If the existence of a document that was previously unknown is referred to in parliamentary hearings for example it becomes a shallow secret. Once a secret becomes shallow it becomes knowable. Perhaps the most famous example of the stripping of layers of secrecy is the revelation of the Watergate tapes'

---

[43] See, D. Pozen, "Deep Secrecy", *Stanford Law Review*, 62(2), 2010, pp. 257-339.See further, K.L. Scheppele, *Legal Secrets. Equality and Efficiency in the Common Law* (Chicago: University of Chicago Press, 1988), p. 21.

[44] See, D.Pozen, op.cit. at p. 257

[45] See, *ibid*., at p. 21

[46] See, *ibid*., at p. 76. See, D.Pozen, op.cit at p. 262.

[47] See further, D. Pozen, *op. cit*. at p.262.

[48] See, D. Rumsfeld, Secretary of Defense, Department of Defense, News Briefing (February 12, 2002). Available at: <www.defense.gov/transcripts/transcript.aspx?transcriptid=2636>.

[49] See, *Rum remark wins Rumsfeld an award*. Available at:

<news.bbc.co.uk/2/hi/3254852.stm>.

[50] See, in general D.Pozen, op.cit.

existence. It was only through its capacity to question a former presidential aide that a US Senate Select Committee discovered the tapes' existence in the first place. Once the tapes became a shallow rather than a deep secret, further legal and political maneuvering could take place in an effort to discover their content.[51]

The regulation of secrecy

Secrecy is a matter of government regulation yet it is generally not regulated on in public.[52] What is different with secrecy as opposed to normal regulations on how citizens must behave is that the public does not necessarily know the extent or the content of the regulation. Secrecy concerns what citizens may know; and the citizen is not told what may not be known.[53]

How does the process of ensuring effective protection of government secrecy work? It rests on two main pillars. First, an official must identify what information is to be kept secret and the rules of classifications and physical security. This will generally be on what is termed national security. Such classification restricts the dissemination of documents or information the disclosure of which would injure national security.

The three best-known classification categories, listing from most to least restrictive are *Top Secret*, *Secret* and *Confidential*.[54] Once information is classified, it is marked accordingly and given various forms of protection – including restricting access to people with a security clearance at the appropriate level, physical protection and restrictions on how it may be transferred from one person to another. The second pillar is to ensure that the secret is shared only with those viewed as trustworthy: a combination of personnel security rules and the principle of "need to know".[55] In addition it is increasingly common for governments (and also international organizations such as the EU, see below) to protect a great deal of information *outside* the formal national security classification system. There is now a whole new category of sensitive but unclassified information (in the US known now as *Controlled Unclassified Information*, CUI[56]) that is difficult to pin down and define, in part because of the greatly varied rationales used to justify its protection.[57] The confusion about why this information is to be protected and how it is to be handled may lead it to being mistaken for a *fourth* classification level, causing unclassified information with these marking levels to be treated like classified information.[58]

As we have seen, secrecy in the personal realm may be crucial for identity formation. In the political or public realm secrecy is however ambiguous and much more problematic. In the words of the *Moynihan Committee* (1997): "Some things should never be made secret. Some things should be made secret, but then released as soon as the immediate need has passed. Some things should be made secret and remain that way. The problem is that organizations within a culture of secrecy will opt for classifying *as much as possible, and for as long as possible*."[59] It must be recognized that classifying

---

[51] See further, H. Kitrosser, "Secrecy and Separated Powers: Executive Privilege Revisited", *Iowa Law Review*, 92(2), 2007, pp. 489-544 , at p. 529.

[52] See, *Report of the Commission on Protecting and Reducing Government Secrecy* (hereafter: the Moynihan Committee) (Washington: US Government Printing Office, 1997), at p. xx1.

[53] See, the Moynihan Committee Report (1997), at p. xxxvi.

[54] See further, on the three classification levels in the US context: Executive Order 13526 of 29 December 2009 on *Classified National Security Information*. Available at: <www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information>.

[55] See further, in general, H. Relyea, "Government Secrecy: Policy Depths and Dimensions", *Government Information Quarterly*, 20(4), 2003, pp. 395-418.

[56] See further, in the US, <www.archives.gov/cui/>.

[57] For the history of the evolution of the category sensitive but unclassified see further, Congressional Research Service, Library of Congress, "'Sensitive but unclassified' and other federal security controls on scientific and technical information: history and current controversy". Available at: <www.fas.org/sgp/crs/RL31845.pdf>.

[58] See too, Moynihan Committee Report (1997), at p. 29.

[59] See, *ibid*, at p. xxxix. Author's emphasis.

too much is a lower risk strategy for public officials than too little and there is little incentive for them not to classify material as well as little control in practice over the substance of overclassification or unnecessary classification. That is why legislation was introduced in the US Congress specifically entitled: "*Reducing Over-Classification Act"* [60] and signed into law in October 2010. [61]

Government departments and agencies operating within a culture of secrecy have two main tools that cause secrecy to multiply quasi-automatically: the principle of derivative classification and the principle of originator control. Most information is in fact classified by a process known as *derivative* classification[62]. This process effectively gives the power of secrecy classification to any persons who are cleared to see documents in the respective classification categories. Thus any of the persons who have Top Secret classification clearances are empowered to create Top Secret documents. Whenever a person uses for example a Top Secret source in preparing a *new document* they are obliged to classify the new document according to the classification of the source of information. Since documents must carry the highest classification of their component parts any document which uses a Top Secret source can itself be classified Top Secret. However, since classification is typically both anonymous and nonspecific, a user of a Top Secret source has no way of knowing what particular piece of information led to it being classified Top Secret. As a result the derivative classifier will apply a Top Secret Classification to her document if she has used any information whatsoever from a Top Secret source (although that may not in fact be the "Top Secret" bit).

Derivative classification leads very simply and easily to overclassification. The problem of *overclassification* is not a new problem. On the contrary it seems to have been a feature of the classification system almost from the very beginning. During the course of the past sixty years in the US alone there have been no less than eight "major reviews" of the security classification systems precisely because overclassification remains such a problem[63]. It is also *not* a minor problem. Experts' assessments estimate that between 50% to 90% of what is classified is either overclassified or should not be classified at all.[64]

Another aspect leading to the spread of government secrecy is what is known as *'ORCON creep'*[65]. This is not a new horror movie but the acronym for the phenomenon of *'originator control'*. Traditionally, governments have insisted on applying the rule of originator control – ORCON – before they share information with other governments. The ORCON rule allows originating governments or agencies/institutions to retain control over the declassification of information (if it is classified), or its release to non-governmental parties (if it is not). If the information has been classified by State (or

---

[60] <www.fas.org/sgp/congress/2010/hr553.html>.

[61] <www.whitehouse.gov/blog/2010/10/07/president-signs-hr-553-reducing-over-classification-act>.

[62] See further, C.R. Nesson, "Aspects of the Executive's Power Over National Security Matters: Secrecy Classifications and Foreign Intelligence Wiretaps", *Indiana Law Journal*, 49, 1973-1974, pp. 399-421, at p. 402; see too, the Moynihan Committee Report (2007), *op. cit.*, at pp. 31-32, noting that at that time "ninety-four percent of all classification actions in the last six years have occurred when personnel have classified 'derivatively' by extracting or paraphrasing information in already-classified materials, or by using their own interpretation of what they believes requires classification, including the use of classification guides".

[63] See, H. Relyea (2003), *op. cit.*, at pp. 398-410.

[64] See, *Too Many Secrets: Overclassification as a Barrier to Information Sharing: Hearing Before the Subcommittee on National Security, Emerging Threats, and International Relations of the Commmittee on Government Reform House of Representatives*, 108th Cong., at 82 (Aug. 24, 2004) (statement of Carol A. Haave, Deputy Secretary of Defense for Counterintelligence and Security); Donald Rumsfeld, *War of the Worlds*, Wall St. J., July 18, 2005, at A12 (acknowledging "too much material is classified across the federal government as a general rule"). A 2006 audit report of the Information Security Oversight Office found that at least one out of three of more than 25,000 previously open records had been improperly re-classified: *The Media's Role and Responsibilities in Leaks of Classified Information: Hearing Before the House Permanent Select Committee on Intelligence*, 109th Cong., at 1 (May 26, 2006) (statement of Meredith Fuchs, General Counsel, National Security Archive). See too, Statement of T. Blanton to the Committee on the Judiciary, US House of Representatives, 16 December 2010, Hearing on the Espionage Act and the Legal and Constitutional Implications of Wikileaks. Available at: <judiciary.house.gov/hearings/pdf/Blanton101216.pdf>.

[65] See further on this phenomenon, A. Roberts, "ORCON Creep: Information Sharing and the Threat to Government Accountability", *Government Information Quarterly*, 21(3), 2004, pp. 249-267.

Agency) A, it cannot be reclassified or declassified by State B (or an international organization), unless State A consents to the change. Similarly, no information provided by State A can be given by State B (or an international organization) to a third party – such as another government, non-governmental organization or citizen – without the consent of State A.

A similar type of originator control is applied, for example, extensively in the EU context where for documents stemming from third parties or Member State governments the originator outside the EU determines whether access within the EU rules can be given or not.[66] In these circumstances the control by third parties or Member State governments over shared information in the EU context is absolute. There are no norms or review mechanisms that compel that state or private party to justify its decision to refuse a request for declassification or release of information which it has provided to one of the institutions of the European Union.

The ORCON rule eliminates the ability of states/agencies/international organizations to make their own judgments about the wisdom of releasing shared information. In the US context when information is shared 'horizontally' across each level of government and 'vertically' among federal, state, and local governments, private industry, and citizens, originator control applies very widely. In addition there can be no unauthorized disclosure of foreign government information as this "is presumed to cause damage to the national security".[67] What this means is that unclassified information received from foreign governments can be classified by US agencies or other actors on the grounds that the act of disclosure without consent would undermine international relations and thus harm national security.[68]

As the US government responded to the terror attacks of September 11 the influence and remit of the ORCON rule in the domestic/internal sphere has expanded, also by including the ORCON rule in new information sharing policies. In addition, the classification system has been expanded and now includes the protection of *'homeland security'* as an explicit goal. The adaptation of the classification system has involved an expansion in the number and types of officials authorized to receive classified information (including state and local officials incorporated into the federal classification system and having received the necessary security passes). Finally, the new category of sensitive homeland security information ("limited use", "sensitive", etc) is not classified, includes the ORCON rule and is exempt from disclosure from the freedom of information legislation.

The secrecy regulation process has its own particular malignancy and has led to what US Congressman Daniel Moynihan in a 1997 report called "a hidden, humongous, metastasizing mass within government itself."[69] It has led to a vast structure and spread of secret government both in the US and in Europe as well. This vast secrecy mass has grown gigantically since 9/11. It has spread far beyond traditional aspects of national security to embrace police protection, border defence intelligence sharing etc. This is referred to as *'homeland'* or *'internal security'* and can be opposed to national security in the sense of foreign policy and information on foreign governments."Top Secret America" (and later "Top Secret Europe", see below) beckons.

Top Secret America

In July 2010 the *Washington Post* published a series of articles on "Top Secret America" including *a new geography* of what it termed top-secret government in the US.[70] It depicts the scope and complexity of the government's homeland security program through interactive maps and other graphics.[71] It also shows the rapid growth of the USA's heavily privatised intelligence establishment

---

[66] See, for example, Article 4 (5) of Regulation No 1049/2001 of 30 May 2001, regarding public access to European Parliament, Council and Commission documents, http://www.europarl.europa.eu/RegData/PDF/r1049_en.pdf

[67] See, Executive Order 13526 of 29 December 2009, *op. cit.*, at section 1.1(d).

[68] See, A. Roberts (2004), *op. cit.*, at p. 253.

[69] See, D.P. Moynihan, "The Science of Secrecy". Available at: <www.aaas.org/spp/secrecy/Presents/Moynihan.htm>.

[70] See, *Top Secret America. A Washington Post Investigation.* Available at: <projects.washingtonpost.com/top-secret-america/>.

[71] This video link gives a graphic overall impression: <projects.washingtonpost.com/top-secret-america/map/>.

that works in close collaboration with public government.

In the words of the authors:

> The United States is assembling a vast domestic intelligence apparatus to collect information about Americans using the FBI, local police, state homeland security offices and military criminal investigators. The system, by far the largest and most technologically sophisticated in the nations' history, collects, stores and analyzes information about thousands of US citizens and residents, many of whom have not been accused of any wrongdoing.[72]

The Wikileaks cables illustrate that although classification rules are designed to strictly limit who has access to the secret and how, such limitations may in practice be wholly illusory. This has to do with how many people knew, what sorts of people knew, how much they knew and the timing when they knew.[73] Wikileaks revealed huge security failings in the protection of classified material including the fact that an extremely substantial *number of persons* within the US administration had access to such 'secrets'. According to one report more than *3 million* US military and civilian personnel had the security clearance necessary to access the US Defense Department *Secret Internet Router Network* (SIPRNet).[74]

How secret is a secret that 3 million people have access to? Benjamin Franklin already knew the answer to that. As he put it: "Three may keep a secret if two of them are dead."[75] Second, a study of the almost banal contents of some of the classified documents reveals a serious problem of overclassification of material, perhaps because of the application of derivative classification as well as originator control.[76]

Neither one of these problems is new but they do put the spotlight in a more general manner on the way that the US government in particular has expanded government secrecy post 9/11. Such excessive and unwarranted secrecy removes vast amounts of information from public scrutiny, shielding misconduct and impeding oversight. It obstructs citizens ability to seek disclosure of government held information because classified information is generally excluded as such from any freedom of information laws, without any discussion possible as to the accuracy or otherwise of the classification in question. But layers of secret government in democracies are not only found in America post 9/11; their malignant and spreading mass is also growing in Europe and in particular in the context of the supranational European Union.

Top Secret Europe

NATO security standards applied

It is not obvious to apply the same reasoning and analysis on the regulation of secrecy to international organisations given that international organisations generally do not have an independent ability to autonomously gather and process sensitive information on national security. If they do, as with NATO, an organization whose mission is the promotion of collective security, they establish strict rules on the handling of classified information within the government of its Member States. NATO's security of information policy – crafted in the early days of the Cold War – is tilted towards secrecy to

---

[72] *Ibid*. Available at: <projects.washingtonpost.com/top-secret-america/articles/monitoring-america/>.

[73] See further on this categorization, D. Pozen (2010), *op. cit.*, at pp. 267-268.

[74] See, *Wikileaks Breach Highlights Insider Security Threat.* Available at:

<www.scientificamerican.com/article.cfm?id=wikileaks-insider-threat>, citing a GAO report from 1993, although it remains unclear as to how many people actually have roles that allow them the clearance to access SIPRNet.

[75] B. Franklin, quoted in the Moynihan Committee Report (2007), *op. cit.*, at p. 4.

[76] This was a problem the Moynihan Committee already referred to.

what some claim is an unwarranted degree.[77] The ORCON principle applies[78], as does the derivative principle. Even NATO unclassified information "can only be used for official purposes" and may not be released under national freedom of information laws.[79] This includes the security rules themselves which although "unclassified" may not be made public.[80] The depth of coverage of the NATO rules are arguably more extensive than the US classification since they include a fourth and lowest category of RESTRICTED applicable to information whose relevance to security is negligible, if its disclosure would be "undesirable to the interests of NATO."

NATO procedures have had a controversial impact on the European Union's policy concerning access to documents. Just two months prior to the adoption of the EU access to documents legislation,[81] the Council of Ministers adopted in March 2001 new security regulations governing EU classified information. These rules, together with the exclusions on "sensitive documents" contained in the EU access regulation, ring fenced almost all classified information and excluded it from public access provisions (although in the EU rules dating from 2001 there is no RESTRICTED information[82]). These security rules replicate to a large extent NATO security rules except that in the EU security rules there is no RESTRICTED information.

The Council's decision explained that the EU's expansion into the field of defense policy would require the exchange of "particularly sensitive" information, and that this could be accomplished "only if the originator of such information can be confident that no information put out by him will be disclosed against his will. "[83] At the same time the Secretary General of the Council had entered into an interim security agreement with NATO that incorporated the key elements of NATO security policy.[84] The span of these security regulations is not limited to EU institutions: Member States also are placed under an obligation to adopt "appropriate national measures" to ensure that the Council's rules on the handling of classified information are respected within their governments. This led in particular to a spate of new state secrets laws in newly joined Eastern European Member States.

The drive to promote collective security has thus produced a thickening web of intergovernmental and supranational commitments on the handling of classified information and unclassified but sensitive information. What is newer however is the emergence of the supranational European Union as a security actor in its own right and in a manner that is closely modelled on evolutions in the US, in particular since 9/11. As a security actor it gathers and processes information autonomously. It also shares information both internally and externally.

In Europe there is however no accessible new geography of top-secret government. The EU is not a state, federal or otherwise, that can as such be compared to the US. Yet the European Union does

---

[77] See, for example, A. Roberts, "Entangling Alliances: NATO's Security Policy and the Entrenchment of State Secrecy", *Cornell International Law Journal*, 26(2), 2003, pp. 329–360.

[78] See, *Security within the NATO*, Note by the Secretary General, Document C-M (2002) 49, 17 June 2002, Enclosure B, 9 (g). Available at:

<www.statewatch.org/news/2006/sep/nato-sec-classifications.pdf>.

[79] See further, A. Roberts, *op. cit.*, at p. 334. This may be compared with the situation under the Western European Union, the security rules of which are made publicly available.

[80] But see the copy made available by NGO Statewatch. Available at: <www.statewatch.org/news/2006/sep/nato-sec-classifications.pdf>.

[81] Regulation (EC) No 1049/2001 of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents, 30 May 2001, OJ L 145/43.

[82] In the amendment to the rules dating from 2009 that still have not been adopted this category is included. See, Proposal for a regulation of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents (recast) (COM(2008)0229 – C6-0184/2008 – 2008/0090(COD)), 11 March 2009, p. 21.

[83] Council Decision amending Decision 93/731/EC on public access to Council documents and Council Decision 2000/23/EC on the improvement of information on the Council's legislative activities and the public register of Council documents, 14 August 2000, (2000/527/EC), OJ L 212/9.

[84] See, A. Roberts (2003), *op. cit.*, at p. 356.

have supranational small 'g' government that is fragmented and scattered but growing all the time.[85] It also has networks of government actors based in the constituent Member States that increasingly interact with the centre and indeed are steered by the centre.

According to the Lisbon Treaty (Article 4 TEU) national security formally remains a matter for the Member States and by implication not for the EU. Yet a common policy on *internal security*, like its external counterpart, is under construction and in accelerated form at the supranational level. Member States have broadly harmonized their approach to police, intelligence and border protection.[86] The EU has created new agencies in these fields and the number of other actors contributing to policy shaping and decision-making has grown in tandem. Its evolution is bit-by-bit and not terribly visible. The new geography is however there and is being increased incrementally all the time.

EU Internal security

The European Union is quietly emerging as a significant security actor in a general sense in its own right. As we have already seen in relation to the US, security is a much broader concept than the classical understanding of the ability to use military force to protect one's state against external invaders and ensure its survival. In the contemporary world there can be threats to security in the form of organized crime, drug addiction, terrorism, corruption, illegal immigration, money laundering etc and these problems can attack the integrity of a state from the inside. Both internal and external dimensions of security are part of the broad rubric of what constitutes security nowadays.

Since the EU is largely internally borderless, Member States tackle protection of the European 'homeland' in common and this is for the most part a highly integrated area of security policy[87]. This process of creating an internally borderless area began with the signing and implementation of the Schengen agreement in 1985 and continues in an accelerated and more integrated fashion after the entry into force of the Treaty of Lisbon in 2010. The new freedom of movement meant that domestic or national security had to be understood more broadly. National borders became internal EU borders and redefined the concept of boundaries. Consequently each Member State had to conceive of internal security as including territory outside its borders.

The Commission's communication on the subject of EU internal security from November 2010[88] is informative on the new geography of Top Secret Europe and how it will take shape in the coming few years. Three points are particularly noteworthy in the context of keeping government secrecy safe. First, more cooperation is envisaged among supranational and national actors across the broad spectrum of internal security. More joint operations, including Joint Investigation teams, involving police, customs, border guards and judicial authorities in different Member States will work alongside Eurojust, Europol and OLAF. More inter-agency cooperation will take place than hitherto was the case both at the supranational level and at the national level.

Second, such cooperation will be supervised by the Standing Committee on Operational Security (known by its French acronym COSI), newly established in the Lisbon Treaty, so as to encourage "increasingly coordinated, integrated and effective operations" between EU agencies and bodies involved in EU internal security (including Europol, Frontex, Eurojust, CEPOL and SitCen). Moreover COSI will be responsible for the Comprehensive Operational Strategic Plan for Police, known by its acronym COSPOL, another component of the EU "alphabet soup" of acronyms.

Third, such enhanced cooperation leads almost inevitably to more sharing of classified and sensitive information and indeed this is explicitly envisaged. In the words of David O'Sullivan, the Chief Operating Officer in the EU's new *European External Action Service*, speaking to a House of Lords Select Committee Inquiry before Christmas 2010: "It is all down to joined up policy making…

---

[85] See further, D. Curtin, *Executive Power of the European Union* (Oxford: Oxford University Press, 2009).

[86] See further, S. Peers, *EU Justice and Home Affairs Law* (Oxford: Oxford University Press, 2011), third edition.

[87] See, M. Davis Cross, *Security Integration in Europe: How Knowledge-based Networks are Transforming the European Union*, (Ann Arbor, MI: University of Michigan Press, forthcoming).

[88] Communication from the Commission to the European Parliament and the Council, "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe", Brussels, 22 November 2010, COM(2010) 673 final.

You need mechanisms which ensure flow of information. Flow of information is probably the most important thing".[89] That flow of information is across entities such as *COSI*, the *Political Security Committee* and the newly established *European External Action Service* (EEAS).

Europe too is now in the process of assembling an intelligence apparatus to assemble and process information about Europeans using SitCen, the *EU Joint Situation Centre*, now located within the EEAS, previously located within the Council General Secretariat and covers both external and internal security.[90] SitCen does not have access to 'raw' intelligence material or operational information but rather information coming from the Member States and open sources. In addition SitCen works together with the EU Military Staff Intelligence Directorate in a Single Intelligence Analysis Capacity (SIAC).

Europol, Eurojust, Frontex and other agencies, as well as national police and military participate in policymaking and operational collaboration on internal security at the European level. In this context it is not surprising that the Council General Secretariat has for some time now been quietly working on achieving a more comprehensive system for protecting classified information within the EU, in particular by persuading separate entities such as Europol but also other agencies to adopt the Council's own security rules in place of their own.[91]At the same time, an agreement among the Member States on a uniform approach to the protection of classified information exchanged in the interests of the EU is about to be signed by the Member States.[92] This means that there is a whole underground barely visible system under construction with no public input possible. ORCON creep is magnified and extended.

Commissioner Malmström, Commissioner for Home Affairs admitted that for the Internal Security Strategy, the EU "took inspiration from the comprehensive approach of the US Homeland Security Strategy".[93] According to some since 9/11 America has been treated as the 28th member of the EU: it enjoys a presence in Europol and Eurojust and has signed a range of international agreements with the EU on internal security matters. This may soon be taken further. Wolfgang Schäuble, as German Interior Minister, put forward the idea of a Euro-Atlantic area of internal security and it is contained in a report drafted by the High-Level Advisory Group on the Future of European Home Affairs Policy (Future Group).[94] Analysts in Brussels and London say that many of the Future Group's ideas are likely to be implemented either by the full European Union or by a subgroup of countries, because they have the backing of top EU governments and the Commission, and because the proposals have already built up so much momentum that it would be hard to derail them.[95]

---

[89] Revised transcript of evidence taken before the House of Lords Select Committee on the European Union, Inquiry on EU internal security strategy, 7 December 2010. Available at: <www.parliament.uk/documents/lords-committees/eu-sub-com-f/ISS/cEUF071210ev3.pdf>.

[90] See, J.van Buuren, "Secret Truth. The EU Joint Situation Centre" :

http://www.statewatch.org/news/2009/aug/SitCen2009.pdf

[91] See, for example, Council of the EU, 5524/10, "Draft Council security rules –Draft declaration by the Council and the Commission on EU agencies and bodies". 19 january 2010, http://www.statewatch.org/news/2010/feb/eu-council-classified-euci-5524-10.pdf

[92] See, Council of the EU, Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union, 13886/09, 6 November 2009 and 9389/11, Signature of the Agreement, 26 April 2011.

[93] C. Mahlstrom, "The EU Internal Security Strategy –what does it mean for the United States", Discussion organized by the Center for Transatlantic Relations, Washington DC, 8 December 2010, Doc. Speech/10/739, quoted by Memorandum by Dr. C. Hillebrand in written evidence to the House of Lords Select Committee Inquiry on the EU Internal Security strategy, at p. 40. Available at: <www.parliament.uk/documents/lords-committees/eu-sub-com-f/ISS/ISScollatedwrittenevidence.pdf>.

[94] Report of the High-Level Advisory Group on the Future of European Home Affairs Policy (The Future Group), "Freedom, Security, Privacy – European Home Affairs is an Open World", June 2008, at p. 10 and 27. Available at: <www.didierbigo.com/students/readings/eu-futures-jha-report.pdf>.

[95] See, J.Barham, "European Union and United States Counterterrorism Cooperation", *Security Management*, http://www.securitymanagement.com/article/european-union-and-united-states-counterterrorism-cooperation-004819

Be that as it may, as a vista for the not so distant future the Commission is busy putting further foundation stones of internal security in place in Europe. Thus, the Commission proposed EU legislation on the collection of 'Passenger Name Records' on flights entering or leaving the territory of the EU[96] – and there is some discussion on whether this should not also include intra-European flights.[97] Moreover, following the signing of the Swift agreement with the US on terrorist financing tracking the Commission is developing a *EU Swift law* enabling the EU to extract and analyse financial messaging data held on its own territory. The system will collect, store and analyze information about thousands of European citizens and residents many of whom have not been accused of any wrongdoing.

This internal security strategy raises many questions as to the application of the rule of law, in particular the protection of personal privacy and other fundamental rights. There is much to say on this subject and voices are already being raised that the EU's drive towards giving flesh to 'internal security' as a European concept rides roughshod over the values of liberty and justice.[98]

The facts at issue in the *OMPI* case and others on the blacklisting of terrorists shows just how entrenched the notion of executive privilege has become within the EU in spite of the fact that the EU constitutional system has a court acting to defend the rule of law and other constitutional values. An important question is on court procedures and in particular the important role that can be played by the Court of Justice in Luxembourg as a constitutional court. Should the courts in Luxembourg be able to request access to classified information that is relevant to cases brought before them? As the EU goes further down the internal security road it can only be expected that the number of cases where this is a relevant question will increase. At the end of the day a court can do nothing to ensure substantive justice if the information on which the blacklisting or other decision is based is classified and also not revealed to the Court. Yet at the European level, it appears that the courts do not accept non-disclosure to them.[99] Thus, in particular in the *OMPI* case on the blacklisting of terrorists by the UN and within the EU context, the Court said clearly that the Council could not base its decision on information that is not revealed to the Court.[100]

Checks and balances

As I see it there are currently two main problems with the manner in which the executive power in the EU decides what to keep secret. *First* and foremost its regulations on secrecy and security are adopted by virtue of its own internal rule-making power (rules of procedure) and are at no time subject to public debate, even if they are in principle subsequently published in the Official Journal. This is not only the case of the Council of Ministers but also of the Commission and of satellite bodies and agencies (e.g. Europol) which may or may not adopt earlier classifications e.g. of the Council. *Second,* further agreements are made at the inter-institutional level by virtue of inter-institutional agreement among a number of EU level institutions in order to agree how information is shared. This hidden layer of rule making adds further details to the manner in which secrecy is being regulated in EU government.

The best response to the dilemma of ensuring that secrecy is democratic is to make certain that there is proper public discussion of the rules that determine *when* secrets shall be kept. "Secrecy is justifiable, only if it is actually justified in a process that itself is not secret. First-order secrecy (in a

---

[96] Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, Brussels, 2 February 2011, COM(2011) 32 final, 2011/0023 (COD).

[97] See, Statewatch, "UK seeking to extend Commission proposal to cover intra-EU flights from the start", http://www.statewatch.org/news/2011/feb/04uk-eu-pnr.htm

[98] See further, E. Guild and S. Carrera, "Towards an Internal (In)security Strategy for the EU?", January 2011, CEPS Paper. Available at: <www.ceps.eu/book/towards-internal-insecurity-strategy-eu>.

[99] See further, in general, C. Eckes, *EU Counter-Terrorist Policies and Fundamental Rights: The Case of Individual Sanctions.* Oxford: Oxford University Press, 2010

[100] Case T-284/08, *People's Mojahedin Organization of Iran v Council (OMPI III)* [2008] ECR II-3487, at para 73

process or about a policy) requires second-order publicity (about the decision to make the process or policy secret)."[101]

What is termed *second order publicity* is thus key to developing a system of checks and balances in a political system. This means at the very least that the rules governing security classification should be debated on in public and in a holistic way apply to the various actors performing tasks and exchanging information at the European level. Part of this debate is the need to ensure a proper balance with the fundamental principle of openness (as reiterated by the Lisbon Treaty) and the citizen's rights of access to documents and the public interest. Despite the changed environment of the Lisbon Treaty and the drive to an internal security area there is little recognition by the executive power itself that the time has come to approach the matter in a different fashion. Part of such EU wide security rules would include an oversight body and specific rules on declassification as well as other more technical rules.

One thing is sure however: if ever more classified and unclassified but sensitive information is created and shared within the EU context by an ever widening array of actors at different governance levels the role that courts and parliaments can currently play in order to ensure that executive power is not being abused in first order secrecy is very limited.

Some progress has undoubtedly been made in recent years at the European level thanks to a pro-active stance by the European Parliament and helped by the new legal situation introduced by the Treaty of Lisbon. For example, Article 218 (10) EU provides that the Parliament "shall be immediately and fully informed at all stages of the procedure" for ratifying international agreements. This has led to the adoption of an inter-institutional agreement with the Council setting out the conditions for access to classified information for a very limited group with the appropriate security clearances.[102]

As the drive towards an ever more integrated and networked European area of internal security increases not only must there be clear publicly debated European wide rules, there must also be a procedure for the declassification of documents and a special EU wide oversight authority. At the same time internal security must not be used as the newest trump card to negate what the Lisbon Treaty describes in fundamental terms as the need to take decisions "as openly and as closely as possible to the citizens" (Article 1 EU). [103]

Concluding remark

There is of course a legitimate domain for government secrecy but times have changed since the Espionage Act was adopted during the First World War and the NATO and other rules at the height of the Cold War. Rules adopted in those different contexts are arguably no longer fit for the information age. Trump cards such as 'national security' and its more modern variant 'internal security' need to be put on the table face up and considered in the light of other more modern aces such as the public interest as expressed in freedom of information legislation around the world. We need to ensure that second order rules on secret keeping by government in all its various forms are adopted in public and after public debate. We need to put in place a system of checks and balances worthy of constitutional democracies in the twenty first century.

At the end of the day executive power must not abuse its privileged position and the other actors in a political system must ensure that they are equipped to provide the requisite countervailing power. They can only do so if the deep secrets or 'unknown unknowns' are moved into shallower waters where some light can penetrate. In my view this is the lesson from Wikileaks: make the system of government secrecy shallower and thus ultimately more legitimate. This is a more lasting legacy for

---

[101] See, D.F. Thompson, "Democratic Secrecy", *Political Science Quarterly*, 114(2), 1999, pp. 181-193.

[102] Inter-institutional Agreement of 20 November 2002 between the European Parliament and the Council concerning access by the European Parliament to sensitive information of the Council in the field of security and defence policy, 30 November 2002, OJ C 298/1.

[103] See further, for a more extensive consideration of secrecy regulation in the context of the EU and the role of the European Parliament in that context as well as for more structural reform suggestions, D.Curtin, *Top Secret Europe*, Inaugeral lecture of 20 October 2011, University of Amsterdam.

the information age rather than a knee jerk reaction that seeks temporary responses in a hardening and widening of criminal law sanctions against moles and their intermediaries.