



UvA-DARE (Digital Academic Repository)

Top secret Europe

Curtin, D.M.

Publication date

2011

Document Version

Final published version

[Link to publication](#)

Citation for published version (APA):

Curtin, D. M. (2011). *Top secret Europe*. (Inaugural lecture; No. 415). Universiteit van Amsterdam. http://www.oratiereeks.nl/upload/pdf/PDF-5066weboratie_Curtin.pdf

General rights

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

Top Secret Europe

Top Secret Europe

Inaugural lecture

delivered upon appointment to the chair of
Professor of European Law
at the University of Amsterdam
on 20 October 2011

by

Deirdre M. Curtin

This is inaugural lecture 415, published in this series of the University of Amsterdam.

Lay-out: JAPES, Amsterdam

© Universiteit van Amsterdam, 2011

All rights reserved. Without limiting the rights under copyright reserved above, no part of this book may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the written permission of both the copyright owner and the author of this book.

*Mevrouw de Rector Magnificus,
Mijnheer de Decaan,
Collega's van de Universiteit van Amsterdam,
Zeer gewaardeerde toehoorders¹*

On 22 June 2006, the *New York Times* revealed the existence of a secret Bush administration programme initiated weeks after the 9/11 attacks.² This secret *Terrorism Financing Tracking Program* (TFTP) enabled US counter-terrorism officials to gain access to financial records of individual citizens in the US, Europe and beyond. This programme went far beyond earlier initiatives to access financial data for security purposes. It enabled US security officials to 'follow suspicious financial trails around the globe...without having to seek assistance from foreign banks.'³ Such financial analyses promise a 'smart' form of targeting that mirrors and complements the logic of targeted killings and drone attacks.⁴ The large-scale data 'trawling' involved relies heavily on social networking analysis, which looks for underlying connections between people.

All the data requested by the US Treasury were provided by SWIFT in a so-called black box. SWIFT is a Brussels-based consortium, formally known as the Society for the Worldwide Interbank Financial Telecommunication, and it handles about 80% of all financial transfers worldwide, the bulk in Europe.⁵ Instead of seeking individual court-approved warrants or subpoenas to examine specific transactions, US government officials relied on extremely broad non-individualised administrative subpoenas for millions of confidential banking records supplied by SWIFT. US Treasury subsequently mined and analysed the black-boxed data on the basis of specific search queries.⁶

The SWIFT case is exemplary for the manner in which notions of security, both external and internal, are evolving through novel deployments of data analysis that exceed what is conventionally understood as surveillance.⁷ But it is also illustrative of what can be called deep government secrecy – in this case about the very *existence* of the TFTP programme. Deep secrecy is secrecy the existence of which is *itself* a secret.⁸ Deep secrecy breeds leaks by government officials. Dissatisfied 'insiders' may leak documents for a variety of reasons, including concern at the fact that far-reaching decision-making is taking place in secret. Once the existence of the TFTP programme was revealed, the fact

that it had functioned in what was effectively a law-free zone and a politics-free zone was exposed. The Belgian Privacy Commission subsequently found that SWIFT had breached Belgian and European privacy laws by providing the information in question.⁹ There was an outcry at the time in the European Parliament that the US was secretly using confidential banking information of Europeans and infringing their rights to privacy wholesale and in an uncontrolled manner. Later significant safeguards were built into the system in an international agreement between the EU and the US on the exchange of such data from Europe to the US.¹⁰ This was agreed after the SWIFT server moved back to Europe.

The sting in the tail to this whole story however is that exactly ten years after the secret introduction of this surveillance programme in the US, the EU is in the process of introducing its own parallel *Terrorist Financial Tracking System* in Europe – an EU TFTS. The envisaged system will collect, store and analyse information about thousands of European citizens and residents many of whom have not been accused of any wrongdoing. This summer the Commission adopted a communication on the subject outlining a number of options, including the option of attributing the core functions to EU institutions.¹¹ The EU executive and legislative process is not secret but it does suggest a definite parallel between evolving EU *internal security* and US *homeland security*. Part of the EU internal security map is a growing role for intelligence-type agencies and the enhanced sharing of classified information. This makes the issue of secrecy regulation in relation to the EU particularly salient. Let me now look at the conceptual question: what does secrecy mean?

Inside out and Outside in

Questions of secrecy are not new. Secrecy is inherently human. 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.¹² It may be shared with no one or confided to some on condition that it goes no farther. Basic human nature dictates the likelihood that if three people are put together, sooner or later, likely as not, two of them will be keeping some sort of secret from the third.

Scholars have struggled with the general concept of secrecy for centuries. Sociologists have stressed 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.¹³ Or as Harvard philosopher Sissela Bok put it many years ago: ‘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 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.¹⁴

Secrecy presupposes *separation*, a setting apart of the secret from the non-secret, and of keepers of a secret from the excluded targets. 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.'¹⁵ 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.¹⁶ Moving from the personal to the public, Simmel argues that secret keeping actually endows secrets with *value*.¹⁷ 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'.¹⁸ 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*.¹⁹ In the personal realm, secrecy may be crucial for identity formation but in the political or public realm, secrecy is ambiguous and much more problematic.

Donald Rumsfeld as US Secretary of State for Defense had this to say on the structure of secrets in the public realm:

'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 one'.²⁰

Almost from its moment of utterance – in 2002 – commentators ridiculed Rumsfeld for his 'kabbalistic logic and professorial cant'.²¹ The British Plain English Campaign called it 'the most nonsensical remark made by a public figure'²² in memory. Yet the secrets or things we do not know we do not know are indeed the most difficult ones for a free society. The deeper the secret, the fewer the people who will know the secret.²³ When a small group of similarly situated officials conceals from outsiders the fact that it is concealing something, the result is a *deep secret*.²⁴ Deep secrets may more often involve bad

faith or fraud.²⁵ 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.

According to a 2010 Washington Post exposé called ‘Top Secret America’ an estimated 854,000 people hold top-secret security clearances in the US and an estimated 2.4 million hold security clearances at the confidential, secret and top-secret levels.²⁶ ‘Deep’ and less deep secrecy is thus a relative notion in terms of exact numbers of insiders and outsiders. Yet, even apparently deep secrets may be known by complete outsiders. In the case of the TFTP and SWIFT the European Central Bank apparently knew of the existence of the programme and SWIFT’s role in supplying data to the US authorities *before* the New York Times went public. They too kept this US secret *secret* despite the implications for the privacy of Europeans.²⁷

The concepts of deep and shallow secrets can best be illustrated 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.²⁸ When members of the general public or of oversight institutions understand that they are being denied particular items of information, the result is a *shallow secret*. Information which has been classified but the existence of which is not hidden (either in document registers or otherwise) is a shallow secret. A shallow secret may be challenged by procedural or other means. Deep-secret keepers will generally be more concerned to conceal from the target the fact that they wish to conceal something than shallow-secret keepers.²⁹

As government secrecy grows and comes to involve more people, the opportunities to leak from within expand. The more ‘insiders’ with access to the secret, the more likely a secret will leak out. The fact is that government officials leak classified information all the time – to influence policy, take credit or deflect blame. Bradley Manning, the US government official who allegedly leaked the over 250,000 documents to Wikileaks, was reportedly motivated by a desire to expose secret government activities to public scrutiny.³⁰ Perhaps the most famous example, however, of the stripping of layers of secrecy is the revelation of the Watergate tapes’ 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 manoeuvring could take place in an effort to discover their content.³¹

From national security to EU internal security

Dispersed threats to national security inside out and outside in

What is the underlying rationale for government secrecy in the first place? As John Jay wrote in *The Federalist* the executive might sometimes need ‘perfect secrecy’.³² Traditionally, some amount of secrecy is considered valuable for concealing plans and vulnerabilities from adversaries, for acting quickly and decisively against threats, protecting sources and methods of intelligence gathering and investigating and enforcing the law against offenders.³³ A similar line of argument was classically used to support secrecy in international negotiations and in diplomacy more generally. In addition to what can be termed the national security rationale for government secrecy there is also a more *administrative* rationale for government secrecy.³⁴

National security is *the* key justification traditionally given for classifying documents as confidential, secret and top secret and there is a tendency to regard national security as a trump card in this respect.³⁵ Thus, 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’.³⁶ It is often assumed that the protection of sources and methods of intelligence collection and analysis must be kept secret (classified) because they are vulnerable to countermeasures. Like Russian dolls, secrecy to protect sources and methods nests within the collection and development of useful intelligence which, in turn, nests within the development of national security policy. Secrecy in this way becomes what US Congressman Daniel Moynihan described in 2007 as ‘a hidden, humongous, metastasizing mass within government itself’.³⁷

National security (or ‘foreign policy’ as the more general term covering foreign, security and defence policy) traditionally had an explicit *target* in the sense of a party against whom a government is taking action. Publicising information about these policies posed a special risk of ruining the underlying objective.³⁸ As we have already seen however in relation to the US and the SWIFT affair, security nowadays 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 organised crime, drug addiction, terrorism, corruption, illegal immigration, money laundering, etc and these problems can attack the integrity of a state from the *inside*. Moreover the ‘threats’ to security have become increasingly transnational in nature and also increasingly ‘networked’ and thus dispersed.³⁹ The TFTP referred to earlier on has to

be understood in this context and makes the turn to the network analysis of commercial and financial data easier to place. However, the SWIFT case also shows that the distinction between internal and external security becomes increasingly difficult to draw.⁴⁰

How does this changed understanding of security relate to international cooperation among States? 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 organisation 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 what some claim is an unwarranted degree.⁴¹ Is this true too for the EU? Prior to looking squarely at how secrecy is actually regulated within the EU context it is relevant to consider the underlying rationale for government secrecy – national security – in that context. Without at this point engaging in an existential discussion on the nature of the EU – international organisation, federal would-be state or polity *sui generis* – let me draw out some general lines in the relatively recent evolution of the EU as a political union that have made the issue of secrecy particularly salient and which illustrate how the external and the internal dimensions of security have come together in this context too.⁴²

EU security actors: from policy advice to policy making?

The European Union is quietly emerging as a significant security actor in its own right.⁴³ As a security actor the EU gathers and processes information autonomously. It also shares information both internally and externally. Formally speaking, national security remains a matter for the Member States and by implication not for the EU (see, Article 4 TEU). However, since the EU is largely internally borderless, Member States tackle protection of the European 'homeland' in common and this 'homeland' is for the most part a highly integrated area of security policy. 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 2010.⁴⁴ Freedom of movement within the EU meant that geographically 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 its own internal security as including territory outside its borders.⁴⁵

EU policy on its own 'internal' security is taking shape bit by bit and in an accelerated fashion over the course of the past few years. The Stockholm programme, the five-year strategic work programme for the Area of Freedom Security and Justice (AFSJ), called upon the Council and the Commission to 'define a comprehensive Union internal security strategy.'⁴⁶ The link and complementarity between internal and external aspects of EU security is an important red thread, running through all the relevant core documents on internal security. With much of the organised crime threats to internal security originating outside the EU⁴⁷ this is clearly a highly relevant aspect. As observed by the EU Home Affairs Commissioner in her evidence before the House of Lords, 'threats are not exclusively internal or external but interlinked.'⁴⁸ The relevance of this link for the operational-cooperation work of various EU actors is also acknowledged.⁴⁹ It poses a particular problem in the context of the new European External Action Service where a focus only on the 'external' does not work.

Agencies such as Europol and Frontex are not foreseen to become policy-makers in their own right or to replace the Commission, the Member States or the Council in this regard. Whereas these (and other) agencies have a specific role in the internal security policy process (their threat assessments will inform political priority-setting and policy in the area), they are not envisaged to set priorities or make policy. However, the dividing lines between policy advice and actual policy-making can become blurred in practice particularly given the close link between threat assessment, political priority-setting and ensuing policy choices; this creates possibilities for agencies to influence and shape future policy.

Of course, these EU actors can be distinguished from what are generically termed intelligence agencies at the level of the Member States themselves since the EU actors have no 'special powers' to collect information, such as the powers to intercept communications, conduct covert surveillance, use secret informants, etc. A very important similarity between national intelligence agencies and the EU actors is, however, that they receive, produce and disseminate classified information. They collect, analyse and disseminate information – on threats to internal security or other interests – to policy makers and other executive bodies. They perform these functions both within the territory of the EU and in its relations with third countries and international organisations.⁵⁰ If one looks at, for example, the Commission proposals on the EU TFTP one can only be struck by the fact that across the various institutional options a pivotal role is envisaged for various EU actors and agencies.⁵¹ Can EU institutions, agencies and other actors collect, analyse and disseminate classified information despite national security remaining formally a matter of compe-

tence for the Member States? Let us now look closer at the multiplicity of actors involved.

Internal and external relations of EU agencies: an opaque map

In the new EU internal security strategy more inter-agency cooperation across the broad spectrum of internal security will take place than hitherto was the case both at the supranational level and at the national level.⁵² This means more joint operations, including Joint Investigation teams, involving police, customs, border guards and judicial authorities in different Member States who will work alongside Eurojust, Europol and OLAF. More cooperation among agencies and other actors leads almost inevitably to more sharing of classified and sensitive information and indeed this is explicitly envisaged and builds on what already takes place. Thus the operational agreement signed between Europol and Eurojust in 2004 provides for the exchange of operational, strategic or technical operation and even personal data.⁵³ In 2008 a secure communication link was established to facilitate the exchange of information. The two agencies also agreed on a table of equivalence to exchange classified information above the level of 'restricted'. There are also other strategic agreements including some information exchange between Europol and other actors, for example the Commission and the European Central Bank⁵⁴ and also Frontex.⁵⁵

Internal security cooperation is supervised by the Standing Committee on Operational Security (known by its French acronym COSI). It was newly established in Article 71 TFEU as part of 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, and SitCen, the EU Joint Situation Centre). Moreover, COSI is responsible for the Comprehensive Operational Strategic Plan for Police, known by its acronym COSPOL, another component of the EU 'alphabet soup' of acronyms.

EU agency cooperation takes place not only on aspects of internal security but also on related *external security* aspects. Individual agencies have clearly developed this dimension of their work. Europol for instance, has established over the years bilateral agreements in around thirty cases, with a full-blown operational agreement, allowing for the exchange of personal data, in ten of those cases.⁵⁶ Similarly, Eurojust has built on its external reach through a multitude of external cooperation agreements⁵⁷ with third parties/countries as well as through the presence of external liaison prosecutors at Eurojust premises

(e.g. Norway, Croatia, the US). With regard to joint agency cooperation vis-à-vis third countries, however, this is reportedly limited.

That flow of information is across entities such as COSI, the *Political Security Committee* and the newly established *European External Action Service* (EEAS). SitCen, located now within the EEAS does not have access to ‘raw’ intelligence material or operational information but rather to information coming from the Member States and open sources.⁵⁸ SitCen covers both external and internal security and the fact that it is now nested within the EEAS means that the latter too conflates internal and external security in a structurally opaque fashion. SitCen definitely falls short of being a EU Intelligence Agency like the CIA, but it is gradually becoming a more robust and central element in the EU’s internal-external security nexus, especially in the light of the Lisbon Treaty.⁵⁹ All of these actors share classified information both within the EU and outside the EU. How do these evolving practices fit within the broader structure of secrecy regulation in the context of the EU? Let us now look specifically at how these rules have evolved.

The secrecy regulation process: a first cut

From 1958 to 1992: a subterranean classification system

Traditionally decision-making in the Council of Ministers was behind closed doors to allow the Member States to conduct diplomatic negotiations. This inevitably entailed some sharing of information, even from the very early days, and the creation of documents at the European level. The first rules on the classification of documents for security reasons date already from 1958 when the Council of the European Atomic Energy Community (Euratom)⁶⁰ gave the supranational Commission a classification and supervisory role over ‘Euratom Classified Information’ (hereafter: ECI) as well as establishing a security vetting infrastructure. The security gradings for ECI were from the very beginning *four* fold: Top Secret, Secret, Confidential and Restricted. The latter security level – Restricted – is an additional one compared to what was (and still is) common in the US and many other democracies but reflects long-standing NATO practice. This lowest level of classification (for which no special authorisation for access is necessary) was required ‘where unauthorised disclosure would *affect the defence interests of one or more Member States*.’⁶¹ 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.

ECI covers 'information acquired by the Community or communicated by the Member States which is covered by Articles 24 and 25 of the Treaty establishing the European Atomic Community.'⁶² EU classification rules applied from the very early days of European integration to both relevant Member State documents and other more autonomous Community level information. The link with Member State documents and the limit on national executive discretion to grant public access and or declassify was reinforced – twenty-five years later – in the general Archives regulation of the European Community (1983).⁶³ *Member States* could not release through national archives to the public on terms less strict than those in the Archives regulation (i.e. 30 years) 'documents and records emanating from institutions and physically held in their public archives, which have been classified and have not been declassified.'⁶⁴ This rule also applied to such documents and records of the Member States that reproduce in full or in part the content of such classified documents. In this way, via the Archives regulation, it became clear that what was initially only applied to specific Euratom documents had in fact a more general application.

It took almost forty-five years after the Euratom classification decision for the subject of classification of documents to re-emerge squarely again, this time at the level of the EU as such. Just over two weeks after the Treaty of Maastricht was signed, the Commission proposed a Council regulation on the security measures applicable to classified information produced or transmitted in connection with EEC or EURATOM activities. This sought to widen the scope of the rather subterranean classification system that had operated since 1958 to the full width of Community activities and to regulate it openly in a legislative measure with an advisory role for the European Parliament. The main objective was to afford protection to 'sensitive information whose unauthorised disclosure could be detrimental to the essential interests of the European Communities and of Member states.'⁶⁵ The European Parliament was hostile to the draft Council regulation both on grounds of the legal basis proposed which limited its own role as well as by the failure of the Commission to bring forward concurrently a directive on freedom of information.⁶⁶

The proposal was eventually withdrawn for the surprising reason of 'subsidiarity'.⁶⁷ With the benefit of hindsight the shooting down of the proposal by the European Parliament is regrettable both for substantive and procedural reasons. The security gradings proposed by the Commission were only three and did not include the contested NATO-inspired fourth category 'restricted'. Moreover, some emphasis was put by the Commission on the fact that classi-

fication gradings should be necessary, temporary and take into account wider imperatives relating to access to information. Unfortunately for the European Parliament and in spite of the fact that its legislative and other roles have increased dramatically since 1992, its ability to actually openly debate the contents of the EU-wide secrecy regulation have not improved in a procedural sense since the Commission's 1992 proposal. Rather, its role has worsened considerably when the executive institutions (starting with the Council and the Commission) opted to treat the issue of security and classification rules purely as a matter of their own *internal* organisation. Even when the European Parliament much later acquired a treaty-based role, for example in the negotiation processes of international agreements (in the Lisbon Treaty), the executive institutions continued to treat the issue of special access by members of the European Parliament as a matter of (secret) inter-institutional deliberation and agreement – a process which they dominate (see further below).

'Sensitive' documents ring-fenced and expanded

The reason for the Commission and the Council to adopt new internal rules on the security measures applicable to classified information produced or transmitted in connection with European Union activities, was the fact that in the context of the new common foreign and security policy *sensitive documents* would be produced, shared and circulated. The thinking was that the EU's expansion into the field of defence policy would require the exchange of particularly sensitive information, and that this could be accomplished only if the originator of such information could be confident that no information put out by him will be disclosed against his will. Mind you, this was the case since the entry into force of the Treaty of Maastricht in 1993 and it took the Council until 2001 to adopt new security rules on the classification of documents although it had earlier adopted general rules on security clearances for Council officials in the General Secretariat.⁶⁸ The actual catalyst was in fact the planned adoption of new EU legislative rules on access to documents. The Council staged a 'coup d'état' by adopting its own new security rules just two months prior to the new and fundamental public access legislation. At the same time the notion of 'sensitive documents' was successfully introduced into the access law itself.⁶⁹ These new security rules together with the exclusions on 'sensitive documents' contained in the EU access regulation meant that virtually all classified information was excluded from the scope of the law on public access to documents that was eventually agreed in 2001.⁷⁰ The span of the Council's new security regulations was moreover not limited to EU institutions: Member States were placed under an obligation to adopt 'appropriate national measu-

res' 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.⁷¹ In addition in the EU Access law (2001), it was provided in not so veiled terms that the principle of loyal cooperation governing relations between the institutions and the Member States required that Member States 'take care not to hamper the proper application of this Regulation and should respect the security rules of the institutions.'⁷²

In March of this year (2011), almost a decade to the day after the controversial 2001 security rules, the Council adopted the next generation of its security rules and formally launched EUCI (EU Classified Information). These rules emerged at a moment when the planned revision of the access-to-documents law (on the books since 2009) was stalled in what seemed a structural impasse despite the fact that the Lisbon Treaty had introduced a number of salient changes in the legal framework.⁷³ The full access revision process was however re-ignited in September 2011.⁷⁴ The Council's new security rules emerged into the public realm only after adoption and subsequent publication in the Official Journal but they were worked on – in secret – for a period of at least two years in the Council's security committee and then the Antici Group, responsible for preparing the meetings of the EU's ambassadors (COREPER), and then COREPER itself before final agreement at the ministerial level early 2011. These new rules are much more far reaching in terms of scope and width of application than their 2001 counterpart and constitute an excellent illustration of the expanded scope of executive activity in the EU context.⁷⁵

This is not the place for a detailed analysis of the new security provisions but a number of points indicate just how the domain of secrecy regulation has multiplied. The four (NATO) levels of security gradings are now applied well beyond the common foreign and defence realm. From 2011 the justifications for classifying documents includes *in general* terms 'the interests of the European Union' as well as those of 'one or more of the Member States'.⁷⁶ In other words, the EU now has clearly marked out a classification system that applies across the broad spectrum of its activities with no special mention or position given anymore to the Common Security and Defence Policy. This illustrates indeed how the nature of the EU polity has evolved in the decade since 2001 and how much matters of internal security have become inter-twined with external security and the impossibility of separating the two into a separate 'pillar' as was still the case a decade earlier.

The Council no longer even has the pretence to adopt rules only for its own internal organisation. Its explicit strategy, reflected in its decision, is to obtain the commitment by the Commission, by the Member States and by the other

EU institutions, agencies, bodies and offices with its own rules and standards 'necessary in order to protect the interests of the Union and its Member States. Several declarations appended to the decision make this perfectly clear.⁷⁷ In particular, 'the Council and the Commission consider that their respective security rules, and the Agreement between the Member States, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union, together constitute a more comprehensive and coherent general framework within the European Union for the protection of classified information originating in the Member States, in institutions of the European Union or in EU agencies, bodies or offices, or received from third States or international organisations.'⁷⁸ Thus the Council's strategy of achieving a comprehensive general framework for the protection of EUCI right across the spectrum of the actors and the activities of the EU is spelt out in black and white.

The spider and its (internal/external) web

One can refer to the less than upfront process as effectively a type of harmonisation of secrecy by stealth, with the Council as the sophisticated spider weaving an elaborate and often opaque web. Within its reach are various actors linked to its security system by various mechanisms, all negotiated and agreed in secret and only some structurally transparent when agreed. Thus, the Member States signed a binding agreement less than two weeks after the Council adopted its new security rules, guaranteeing in a legally binding fashion that they would protect classified information originating in the 'European Union institutions, or in agencies, bodies or offices established by the latter and provided to or exchanged with the Member States' as well as their own documents provided to or exchanged with EU institutions etc.⁷⁹ In other words, with this agreement became explicit what has been feared for a long time: not only does the EU adopt rules that bind its own institutions, agencies, etc, but even rules adopted as a matter of the internal organisation of the same institutions can lead to the Member States being restricted under their own national law, constitutional or otherwise, and obliged to give primacy to the EU classification rules. The remarkable point about this process is above all the incremental and barely visible manner in which it occurs, never at any stage having been openly discussed and debated.

Let me give two further examples of the width and depth of the Council's secrecy web. Europol is the front-runner among the agencies when it comes to its own classification rules. In 2009 it adopted its own rules on the confidentiality of Europol information.⁸⁰ Europol carried a first impact assessment in

2009 on the Council revised security rules in relation to Europol.⁸¹ It appears to have queried the general applicability of the Council's rules in the light of the particular legal framework of Europol, especially Articles 40 and 46 of the Europol Council Decision.⁸² Nonetheless, it seems that less than two years later Europol, too, had come around to its essentially subservient position within the Council's secrecy web, notwithstanding its particular circumstances.

The second example of how embedded even an institution such as the European Parliament has become within the comprehensive secrecy ambition of the Council is the very recent decision by the Bureau of the European Parliament concerning the rules governing the treatment of 'confidential information' by the European Parliament.⁸³ It, too, is based on the internal rule making power of the institution itself and relies on its own rules of procedure as the legal basis. This extraordinary 'decision' by the bureaucracy of the EP takes over the Council rules on EUCI but at the same time explicitly covers what is termed 'other' confidential information. This term refers to non-classified confidential information and lays down the basic principles and minimum standards. Such 'other' confidential information is part of a whole new category of *sensitive but unclassified information* (in the US known now as *Controlled Unclassified Information*, CUI⁸⁴) that is difficult to pin down and define, in part because of the greatly varied rationales used to justify its protection.⁸⁵ Such information often receives the stamp or grading of 'limited' in the EU context, which is actually not referred to anywhere in the formal security rules but exists *outside* the formal classification system. The confusion about why 'limited' information is to be protected and how it is to be handled may lead to it being mistaken effectively for another classification level, causing unclassified information with this marking level to be treated like classified information.⁸⁶

A further and expanding part of the security regulation creep includes the *external* dimension. This includes a variety of agreements with third states and international organisations. For example, at the same time as the adoption of the 2001 security rules, the Secretary General of the Council had entered into an interim security agreement with NATO that incorporated the key elements of NATO security policy.⁸⁷ In March 2003, an EU-NATO agreement was concluded for permanent relations, which included the exchange of classified information.⁸⁸ This was the first of many 'security-of-information agreements' concluded by the Council as well as administrative arrangements for the lowest classification level. Article 12 of the new Council rules explicitly provides for this exchange of classified information with third states and international organisations and mandates that their classification levels are no less stringent than those laid down in the Council Decision. In this manner the Council is

weaving a sticky web catching other institutions, agencies, Member States as well as third states and other international organisations in its threads. The most recent information available via the Council's online register of documents is that there are twelve permanent security agreements with third states (including the US) and four more under negotiation or not yet implemented (including with Turkey and Russia).⁸⁹ There are three permanent security agreements with other international organisations and one under negotiation as well as a permanent administrative arrangement with the UN, allowing the exchange of EUCI classified at the 'restricted' level only.

Information sharing among a wide variety of internal and external actors takes place without it being clear how such practices relate to the mandate of Article 1 of the Treaty of Lisbon Treaty that decision-making in the EU will be as open as possible. Information sharing can lead to structural intransparency over what information is being shared and may make the issue of responsibility for classification and declassification fuzzy. Entanglement in the sense of a commingling of information that is so deep that it becomes difficult to separate information that was generated internally and information received externally is likely. When information sharing is combined with the two main tools that cause secrecy to multiply quasi-automatically, the principle of derivative classification and the principle of originator control, we can speak of a culture of secrecy.

ORCON creep and overclassification

Equally important to the formal rules adopted by the institutions themselves is whether a culture of secrecy prevails within the institutions or agencies in question. This is often tied up with a phenomenon known as 'ORCON creep'. This is not a new horror movie but the acronym for the phenomenon of 'originator control' that leads to the multiplication of government secrecy.⁹⁰ Traditionally, governments have insisted on applying the rule of originator control before they share information with other governments or international organisations. This 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). Within the context of the EU this rule has been there since 1958⁹¹ but it has mutated and expanded considerably since then. In a nutshell, it provides that if the information has been classified by State (or Agency) A, it cannot be reclassified or declassified by State B (or an international organisation), unless State A consents to the change. Similarly, no information provided by State A can be given by State B (or an international organisation) to a third party – such as another govern-

ment, non-governmental organisation or citizen – without the consent of State A. The ORCON rule thus eliminates the ability of states/agencies/international organisations to make their own judgments about the wisdom of releasing shared information. The requirement to consult the author (the originator) before granting public access or declassifying is deeply embedded within the Council's rules but also features in several places in the access to documents legislation from 2001.⁹²

The other tool that causes secrecy to multiply is the process known as *derivative* classification. This process effectively gives the power of secrecy classification to any persons who are cleared to see documents in the respective classification categories.⁹³ Thus, only the persons who, for example, 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). The principle of derivative classification applies to all levels of classification.

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. Classifying too much is a lower risk strategy for public officials than classifying too little and there is often little incentive for them not to classify material as well as little control in practice over the substance of overclassification or unnecessary classification. 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.⁹⁴ It is also *not* a minor problem. Experts' assessments estimate that between 50% to 90% of what is classified in the US is either overclassified or should not be classified at all.⁹⁵ We do not sadly have the equivalent figures for the EU nor has there ever been a review, major or minor, of the security classification system in the EU and its link with those of the Member States.

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. 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 three *million* US military and civilian personnel had the security clearance necessary to access the US Defense Department *Secret Internet Router Network* (SIPRNet). How secret is a secret that three 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.’⁹⁶ The reality may well be, also in Europe, that thousands of soldiers, analysts and intelligence officers as well as sub-contractors among others get access to huge volumes of classified and sensitive (but unclassified) material.

Democratic Secrecy: the oversight role of the European Parliament

Mechanisms of oversight mediation

The big underlying analytical perspective on executive secrecy is the democratic one. What is the role of executive secrecy in a democracy?⁹⁷ A basic dilemma of accountability is that democracy requires publicity but that some democratic policies (such as counter-terrorism) require secrecy; if they were made public they could not be carried out effectively or at all – at least this is the argument. Secrecy obstructs the standard mechanisms for oversight utilised by democracies – elections, public opinion and deliberation.⁹⁸ This does not mean that secrecy may not be legitimately claimed by democratic governments but it will need to be balanced against the citizens’ right to information in a democracy and democratic decision-making and oversight. The problem is that since the calculation of harm caused by the disclosure of information cannot be undertaken in public without revealing the very information, this task is delegated to the executive. This is like asking the suspect to provide the evidence!⁹⁹

The general mechanism of *mediation* resolves in theory the conflict between democratic oversight and executive secrecy by having citizens delegate the task of oversight to the judiciary and to the legislature. Mediation therefore promises the benefits of oversight without the potentially adverse consequences of having such oversight conducted in public view.¹⁰⁰ But how successful can mediation be in combating the abuse of executive secrecy? From a practical

point of view, the fact that the executive controls in one form or another the security apparatus allows it to limit very concretely the information available to mediators, both parliament and courts.

Judges are unlikely to conduct searching judicial review where the executive claims that disclosure of secret information or documents would harm national security or its equivalent. In such circumstances judges will often limit themselves to using procedural rather than substantive criteria to gauge the legitimacy of executive secrets.¹⁰¹ In Europe, should the courts in Luxembourg for example 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 for example the blacklisting of suspected terrorists or other decision is based, is classified and also not revealed to it. Yet at the European level, it appears that the courts do not accept non-disclosure to them.¹⁰² 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.¹⁰³

The other main avenue of mediation is oversight mechanisms by parliaments or specialised oversight bodies. Parliamentary oversight of security and intelligence agencies and classified information exchanged in that context is well developed both in the US and in Europe. A recent study shows just how varied that can be among the Member States of the EU and a select number of other democracies.¹⁰⁴ It varies from the worst case Ireland, where no classified information is revealed to parliament and no other mechanism exists to get access to classified information, to the bulk of other countries where a range of parliamentary and specialised oversight bodies exist (including the Netherlands, Spain, Germany and Italy). At the EU level the European Parliament is in any event the only parliamentary forum to provide oversight over classified information produced and circulated in particular by security and intelligence agencies under the auspices of the EU as such. Let us look more closely how this oversight function has evolved over time, both as a matter of law and of practice.

EP oversight by inter-institutional agreement

One of the ways that the European Parliament has expanded its own role since the entry into force of the Maastricht Treaty is by using more informal instruments than treaty-level change, in particular inter-institutional agreements.¹⁰⁵

These were initially ‘own initiative’ inter-institutional agreements not explicitly provided for or indeed envisaged in the Treaties. They are informal in this sense but this does not necessarily exclude their being devoid of any legal effects.¹⁰⁶ For example, the European Parliament negotiated a series of informal and institutional agreements with various actors regarding the provision of information to the European Parliament in a structured and mandatory fashion.¹⁰⁷ The European Parliament has moreover put elaborate arrangements in place to ‘receive’ and handle so-called *sensitive information* that may relate to policy areas such as CFSP, internal security and foreign and security policy. In terms of the further public nature of the rule-making on sensitive documents, a provision is made in the access regulation that the rules of the institutions in this regard are to be made public.¹⁰⁸ This could be interpreted as not entailing necessarily an obligation to publish (for example in the Official Journal) but to make ‘public’ if access is requested. The latter, in any event, seems to be the case with regard to the European Parliament. Moreover, it is explicitly provided that the Commission and the Council shall inform the European Parliament ‘in accordance with arrangements agreed between the institutions’.¹⁰⁹ In other words, the access regulation explicitly foresees the adoption of further implementing inter-institutional rules on how ‘sensitive documents’ will be transmitted to the European Parliament in a manner that will not involve them being made ‘public’ but will respect the confidential classification status.¹¹⁰

What is interesting about the institutional arrangements in question is that they involve the European Parliament making arrangements to receive and ‘handle’ sensitive documents as defined in ‘secure reading rooms’ etc as the *quid pro quo* for being informed on the content of in particular the Council’s security and defence policy.¹¹¹ It seems that such inter-institutional cooperation adds rules and specifications to those previously laid down in secondary legislation. Thus, for example, it is provided that one of the interests to be protected by classification is ‘military or non-military crisis management’ (which is not mentioned in the access regulation itself). Initially, provision was made for the President of the European Parliament and a special committee composed of five specially selected members to ‘ask to consult the documents in question on the premises of the Council’.¹¹² More recently it can be deduced from further rule-making within the European Parliament, and in particular by the President, that secure reading rooms have been established on the premises of the European Parliament itself, presumably to the satisfaction of the Council.¹¹³ At the same time, pursuant to further inter-institutional cooperation between the *Commission* and the European Parliament,¹¹⁴ elaborate provision is made for the forwarding of ‘confidential information’ to the

European Parliament.¹¹⁵ This 'framework agreement' adds to ORCON creep with the European Parliament accepting to be bound by the principle of originator control despite the fact that it is under no legal obligation to do so. It is then a small step from this established 'acquis' for the Council to insist on further ORCON within the new inter-institutional agreement it is negotiating with the European Parliament at present.¹¹⁶ This draft inter-institutional agreement extends the principle of originator control very widely, to other EU institutions, offices, bodies or agencies as well as to EU Member States, third States and international organisations.¹¹⁷ It is constitutionally very questionable: an internal inter-institutional agreement attempting to limit the scope of fundamental Treaty provisions, including Article 1 of the Lisbon Treaty which lays down that the Union takes decisions 'as openly as possible'.

The risk is that as a result of the application of the principle of originator control, a very significant part of EU classified information will never be seen by the European Parliament.

EP oversight over international agreements: caught in a trap?

In terms of parliamentary oversight over institutional secrecy and the negotiation of international agreements (typically the executive prerogative within the EU), 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. One of the most significant new powers given to the European Parliament in the Lisbon Treaty is the power to veto the conclusion of international agreements negotiated on behalf of the EU by the executive power (a combination of the Council and the Commission or in some cases the High Representative).¹¹⁸ Moreover, it is explicitly provided that the EP is to be 'immediately and fully informed at all stages of the (negotiating) procedure.'¹¹⁹ In this way, some democratic oversight has finally been introduced over what was hitherto a matter purely of closed diplomatic negotiations at the European level.

Given the highly political type of issues that the EU is currently negotiating with third states or other international organisations, this is a timely and much needed oversight.¹²⁰ It is also the only parliamentary oversight possible where the agreements fall under the exclusive competence of the EU since national parliaments are then inevitably sidelined. But even with the new Treaty provisions the EP has experienced considerable difficulties in practice in getting timely access to classified documents. The executive institutions argue that strict secrecy is required because otherwise their negotiation strategies with the third country would be undermined. Moreover, by invoking NATO stan-

dards the Council and the Commission have opposed to the EP the principle of 'originator control'. As we have already seen this principle entails that the third country concerned can exert the right to oppose the diffusion to the EP of classified information. It is not a mandatory part of binding European law.

The mediation mechanisms are in and of themselves highly dependent on a hidden mechanism that allows democracies to become aware of possible executive abuse of secrecy in a timely fashion: this mechanism can be referred to as 'circumvention',¹²¹ but is more commonly simply known as leaking. Leaking does not rely on the good faith of the executive but rather evades this structural dilemma completely. Leaking has a symbiotic relationship with secrecy. Dissatisfied 'insiders' may leak documents for a variety of reasons, including concern at the fact that far-reaching decision-making is taking place in secret. This happened for example recently with regard to the 'negotiation mandate' for the (still ongoing) negotiation of an international agreement between the EU and the US on the protection of personal data when transferred and processed by 'the competent authorities of the EU and its Member States and the US for the purpose of preventing, investigating or prosecuting crime, including terrorism'.¹²² The negotiation mandate was placed on line late last year by Statewatch, a UK based civil liberties NGO.¹²³

The Dutch Senate subsequently included this document in its own online database as it was already in the public domain. As a result the Commission – rather extraordinarily – explicitly threatened the Netherlands with infringement proceedings for breach of European law (the document in question was eventually removed from the Senate's web site, allegedly because it was no longer up-to-date). The letter by the Minister for Safety and Justice to the President of the Senate was very explicit on the Commission's threat to sue the Netherlands as a result of the action by the Senate. It proves just how seriously the Commission – and the other institutions – take their own internal classification rules and their binding legal effect. Yet, an examination of this negotiation mandate in terms of substance shows that it is in fact quite a very innocuous document. The description given in the negotiation mandate is not operational at all in terms of negotiation 'strategy', and merely outlines in very general terms a reasonably large number of fairly obvious points for experts that need to be addressed. Moreover, in a EU negotiation mandate the parameters and goals of the EU itself are mentioned to the other party. Such mandates do not contain a negotiation 'strategy' as such, nor will actual negotiations have commenced. This resembles more the desire of a bureaucracy not to be bothered by 'outsiders' (in this case the public on whose behalf they may be negotiating provisions that are effectively legislative in nature and affect the rights and interests of citizens).

The classification level of negotiation mandates is 'restricted', yet this level is not mentioned in the specific provisions in the access-to-documents law from 2001 (currently under revision). This classification level is introduced in the internal rules of the institutions themselves and is applied to 'information and material the unauthorised disclosure of which could be *disadvantageous* to the interests of the Union or of one or more of the Member States'. It is not at all clear what would be 'disadvantageous to the interests of the Union' in making public the actual 'negotiation mandate' other than it being disadvantageous to the interest of the institutions in having their own space to negotiate 'diplomatically' as they are used to doing – freed up from the constraints of publicity. The interest of the citizens of the EU who will see their rights and interests directly affected by the subject matter under negotiation does not seem to be factored into the notion of 'the interests of the Union.' This is the case even where what is being negotiated has a constitutional nature and could change the existing rules of the game.

So how vital is democratic oversight in the circumstances by the European Parliament at this moment in time? It is too early to assess how effectively the European Parliament (EP) is actually maintaining oversight over the negotiation and agreement process of international agreements in the new legal situation after entry into force of the Lisbon Treaty and no empirical research has been carried out yet. It is not clear to what extent the EP is fully being given access to classified information and to unclassified but 'sensitive' information.

The EP for its part is clearly keen to reassure the Council and the Commission that it is very serious about the measures it has taken to ensure the security of classified and unclassified but sensitive information which it receives from the executive institutions, as is evident in the new security rules adopted by its Bureau earlier this year.¹²⁴ At the same time the executive institutions do seem to be intent on setting in place a *limited* exchange of classified information with the Parliament. This is witnessed in particular by the insistence first by the Commission last year (2010) and now in draft by the Council this year (2011) that the principle of originator control fully applies, not only to documents produced by third states and other international organisations but also to documents by the more 'internal' EU actors: Member States, other institutions and bodies. This reinforcement of the ORCON principle in the context of the inter-institutional exchange of (classified) material does not augur well for the ability of the European Parliament to carry out its oversight role effectively. The 'trap' was the enticing prospect of more information exchange but the reality was information with much of the 'meat' removed, at least in the context of international agreements being negotiated with third countries where they can insist on the European Parliament not being given access to

many classified documents. In the case of the US, given that all documents relating to foreign 'governments' (powers) are automatically classified, this automatically means that no access will be given to the EP unless the US agrees to declassify – a highly unsatisfactory position for the EP.

With regard to the controversial category of 'sensitive' (but unclassified) documents, the EP is clearly staking a claim as is evident from its own internal rules adopted by its Bureau earlier in 2011. Yet there is a problem here that has to do with the attitude of the executive institutions to their own internal preparatory documents which they feel they must keep secret in the interests of their own decision making process.¹²⁵ A good example of their secrecy reflex in this regard is provided by their refusal in 2009 to give a MEP, Sophie in 't Veld, a copy of a legal service opinion of the Council on the appropriate legal basis to negotiate and conclude a new SWIFT agreement with the US. She challenged their refusal to give full public access on grounds of international relations and court proceedings and legal advice before the courts and the case is still pending.¹²⁶ This raises the key issue whether executive institutions can claim, contrary to existing court case law,¹²⁷ the right to keep their internal opinion on the appropriate legal basis of international negotiations secret. This kind of reasoning refusing access is not so much based on a concern for the equivalent of 'national security' in the EU context but rather on a different rationale for secrecy already commented on by Max Weber – the inherent tendency of bureaucracies to want to keep their internal deliberations secret.¹²⁸ Officials typically view secrecy as the best protection against outside interference in their activities. Recent history in the US in particular has shown the extent to which keeping internal legal opinions secret can be perverted to facilitate wrongdoing and undermine legal accountability.¹²⁹

The future of EU secrecy: uniting law with governance

Worldwide and within the EU transparency is a growth industry even before the advent of the 'Wikileaks world'.¹³⁰ Much less attention is surprisingly paid to the secrecy regulation process especially in the EU and how that impacts not only on increasingly 'fundamental' rights of public access to information but also on the manner it is regulated at the national level. This lecture aims to put the issue of secrecy and the EU squarely on the map in and of itself at what is felt to be a particularly salient moment in its development towards a 'political' union – that of increasingly dense cooperation both internally and externally constructing and reinforcing a European area of 'internal security'. In this perspective the fact that there is a growing number of actors both inter-

nally and externally sharing (classified) information and adopting their own rules on the basis of their internal organisation power is seen as problematic and as *de facto* undermining parallel constitutional level developments, such as the drive for ever more open decision-making as laid down in the Treaty of Lisbon. There is of course a case to be made for a limited sharing of such information but the policy and limits should be upfront. Secrets can be protected more effectively if government secrecy is reduced overall.

My conclusion from the preliminary analysis I have undertaken is two fold. First, the time is more than ripe to treat the issue of secrecy regulation in and of itself seriously. This means in my view that it must be regulated at the legislative level and across the spectrum of EU activities and no longer as a matter of internal executive prerogative. I believe that the contours of the classification system should be laid out in a *separate* legislative measure and not as part of the public access legislation.¹³¹ Its relationship with the public access law and other laws (such as data protection etc) should then be explicitly discussed and openly regulated. This entails the normal legislative process and co-decision by the EP. Issues such as declassification processes, periodic classification review, classification oversight and extending declassification authority beyond the originator can then be systematically and structurally regulated in a manner that does justice both to the need for executive secrecy and for more openness as constitutionally prescribed. 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 process or about a policy) requires second-order publicity (about the decision to make the process or policy secret).'¹³²

My second set of conclusions is in terms of a research agenda for more mapping of the secrecy phenomenon and the various actors and their intricate inter-relationships as well as the need for more empirical research. The latter is of course tricky when the subject matter is 'secret'; nonetheless, step by step, by means of interviews and otherwise much more can be done than to date to bring the role various actors play, their attitudes and practices out of the dark and (more) into the light. This lecture has very largely focussed on shedding some light on the role *public* actors play in the secrecy regulation process and practice; what is even more in the shadows is the role played by *private actors* and the manner in which that role should be subject to some public regulation. This refers not only to private actors such as SWIFT whose data is used by public actors but also those private actors who are contractors or sub-contractors to EU public actors and in that context have access to classified material.

A law and governance approach can not only shed some more sunlight on hidden actors and processes but also pro-actively design institutional and legal guarantees. In the 'Wikileaks world' we now live in these are urgent challenges that require a pro-active and systemic approach, rather than the current reactive and *ad hoc* one. We need, also in the context of the EU, to take the need for government secrecy seriously but at the same time narrow down what genuinely needs to be protected and move 'deep' secrets into shallower waters. 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.

Notes

1. This constitutes an expanded version of my Inaugural Lecture spoken on 20 October 2011, with full citation references. All websites were last checked on 8 October 2011. The author would like to express her thanks to Angela Moisl and Niki Frenczen for their invaluable help and support in producing this text
2. Lichtblau, E. and Risen, J., 'Bank Data is Sifted by US in Secret to Block Terror', New York Times, online edition, 23 June 2006, <http://www.nytimes.com/2006/06/23/washington/23intel.html?pagewanted=1>
3. Meyer, J. and Miller, G., 'Secret US Program Tracks Global Bank Transfers', Los Angeles Times, online edition, 23 June 2006, <http://articles.latimes.com/2006/jun/23/nation/na-swift23>
4. See further, Amoore, L. and de Goede, M., 'Risky Geographies: Aid and Enmity in Pakistan', *Environment and Planning D: Society and Space*, 29(2), 2011, p. 193-202
5. See, <http://www.swift.com>
6. See further, Wesseling, M. de Goede, M. and Amoore, L., 'Datawars beyond Surveillance: Opening the Black Box of Swift', *Journal of Cultural Economy*, forthcoming 2012
7. See, de Goede, M., 'The SWIFT affair and the Global Politics of European Security', *Journal of Common Market Studies*, forthcoming 2012; and more in general, de Goede, M., *Speculative Security: The Politics of Pursuing Terrorist Monies*. Minneapolis: University of Minnesota Press, forthcoming 2012
8. Pozen, D., 'Deep Secrecy', *Stanford Law Review*, 62(2), 2010, p. 257-339
9. Belgian Privacy Commission, 'Opinion on the transfer of personal data by the CSLR Swift by virtue of UST (OFAC) subpoenas', opinion No 37/2006 of 27 September 2006, Unofficial translation of the Secretariat of the Commission
10. See, Council Decision of 28 June 2010 on the Conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, *Official Journal of the European Union*, L 195, 27 July 2010, at p. 1
11. European Commission, Communication from the Commission to the European Parliament and the Council, 'A European terrorist finance tracking system: available options', COM (2011) 429 final, 13 July 2011, http://ec.europa.eu/home-affairs/news/intro/docs/110713/1_EN_ACT_part1_v15.pdf
12. See, Bok, S., *Secrets. On the Ethics of Concealment and Revelation*. New York: Pantheon Books, 1982, at p. 5
13. See in particular, Simmel, G., 'The Sociology of Secrecy and of Secret Societies', *The American Journal of Sociology*, 11(4), 1906, p. 441-498
14. See Bok, S., *op. cit.*, at p. 24
15. *Ibid*, at p. 5-6
16. *Ibid*, at p. 282
17. See, Simmel, *op. cit.* at p. 464

18. Ibid, at p. 464
19. See further, Bok, S., 1982, *op. cit.*, at p. 172
20. See, Rumsfeld, D., Secretary of Defense, Department of Defense, News Briefing, 12 February 2002, www.defense.gov/transcripts/transcript.aspx?transcriptid=2636
21. These are the words of Pozen, D. *op. cit.* at p. 259
22. See, 'Rum remark wins Rumsfeld an award', BBC News, 2 December 2003, <http://news.bbc.co.uk/2/hi/3254852.stm>
23. See, Pozen, D., 'Deep Secrecy', *Stanford Law Review*, 62(2), 2010, p. 257-339; See further, Scheppele, K.L., *Legal Secrets. Equality and Efficiency in the Common Law*. Chicago: University of Chicago Press, 1988, at p. 21
24. See further, in general, Pozen, 2010, *ibid.*
25. See, *ibid.*
26. See, 'Top Secret America. A Washington Post Investigation', *The Washington Post*, online edition, <http://projects.washingtonpost.com/top-secret-america/>
27. See, Wesseling et al., forthcoming 2012, *op. cit.*
28. See Pozen, D., *op. cit.* at p. 262
29. See Pozen, D., *ibid.* at p. 263
30. See, Bradley Manning in His Own Words: 'This Belongs in the Public Domain', *The Guardian*, 1 December 2010, <http://www.guardian.co.uk/world/2010/dec/01/us-leaks-bradley-manning-logs>
31. See further, Kitrosser, H., 'Secrecy and Separated Powers: Executive Privilege Revisited', *Iowa Law Review*, 92(2), 2007, p. 489-544 at p. 529
32. Jay, J., 'The Powers of the Senate', *Federalist Paper*, 64, 1788
33. See further, Pozen, D., *op. cit.*
34. See further on this rationale, Curtin, D., 'Keeping Government Secrecy Safe: Beyond Whack-a-Mole', Max Weber Lecture Series, July 2011, <http://cadmus.eui.eu/handle/1814/6958>
35. See, Roberts, A., 'National Security and Open Government', *Georgetown Public Policy Review*, 9(2), 2004, at p. 69-86
36. 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. See, <http://www.nist.gov/director/foia/#ex1>
37. See, Moynihan, D.P., 'The Science of Secrecy', <http://www.aaas.org/spp/secrecy/Presents/Moynihan.htm>
38. See, Pozen, *op. cit.*, at p. 275
39. See, in general, Born, H., et al., *International Intelligence Cooperation and Accountability*. Routledge: London, 2011
40. See also, Burgess, P.J., 'There is No European Security, Only European Securities', *Cooperation and Conflict*, 44(3), 2009, p. 309-328
41. See, for example, Roberts, A., 'Entangling Alliances: NATO's Security Policy and the Entrenchment of State Secrecy', *Cornell International Law Journal*, 26(2), 2003, p. 329-360

42. See also, Bickerton, C., et al., 'Security Co-operation Beyond the Nation-State: The EU's Common Security and Defence Policy', *Journal of Common Market Studies*, special issue, 49(1), 2011, p. 1-21
43. See further, Davis Cross, M., *Security Integration in Europe. How Knowledge-based Networks are Transforming the European Union*. Ann Arbor: University of Michigan Press, forthcoming 2012
44. See further, Peers, S., *EU Justice and Home Affairs Law*. Oxford: Oxford University Press, 2011
45. See further, Davis Cross, M., forthcoming 2012, op.cit.
46. The Stockholm Programme – An open and secure Europe serving and protecting the citizens', Official Journal of the European Union, C 115, 11 May 2010, at p. 17
47. See for instance, Europol's EU Organised Crime Threat Assessment (OCTA), 2009
48. Malmström, C., 'Inquiry on EU Internal Security Strategy', Unrevised transcript of evidence taken before the Select Committee on the European Union, House of Lords, 6 December 2010, at p. 6
49. Busuioac, M., and Curtin, D., 'The EU Internal Security Strategy, the EU Policy Cycle and the Role of (AFSJ) Agencies. Promise, Perils and Pre-requisites', Briefing note, Brussels: European Parliament, Directorate General for Internal Policies, 2011, http://www.europol.europa.eu/meetdocs/2009_2014/documents/libe/dv/01_study_eu_iss_/01_study_eu_iss_en.pdf
50. Wills, A. and Vermeulen, M., 'Parliamentary Oversight of Security and Intelligence Agencies in the European Union', Brussels: European Parliament, Directorate General for Internal Policies, 2011
51. See, in particular, the Annex to the Commission Communication, (2011) op. cit., note 11, 'Tabular overview hybrid options', at p. 13
52. 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', COM (2010) 673 final, Brussels, 22 November 2010
53. See, <http://www.eurojust.europa.eu/official-documents/Agreements/Europol-EJ-agreement.pdf>
54. See further, <https://www.europol.europa.eu/content/page/eu-institutions-133>
55. With regard to Frontex, Europol has a strategic agreement, which will in the future turn into an operational one, as Frontex will be able to exchange personal data soon, once its new regulation come through. See for the text, <https://www.europol.europa.eu/sites/default/files/flags/frontex.pdf>
56. For an overview see, www.europol.europa.eu/index.asp?page=agreements
57. For an overview see, www.eurojust.europa.eu/official_documents/eju_agreements.htm
58. This is also envisaged in the Commission's Communication, COM (2010) 673 final, at p. 3
59. See also, Davis Cross, M., 'EU Intelligence Sharing and the Joint Situation Centre: A Glass Half Full?', paper presented at the 2011 meeting of the European Union Studies Association, 3-5 March 2011, http://www.euce.org/eusa/2011/papers/3a_cross.pdf

60. Regulation No. 3 implementing Article 24 of the Treaty establishing the European Atomic Energy Community, Official Journal of the European Union, L 17, 1958, p. 406-416
61. Article 10(4) of Regulation No. 3, *ibid.* Author's emphasis
62. Article 1(1) of Regulation No. 3, *ibid.*
63. Council Regulation (EEC, Euratom) No. 354/83, 1 February 1983, concerning the opening to the public of the historical archives of the European Economic Community and the European Atomic Energy Community, Official Journal of the European Union, L 43, 1983, p. 1-15 (hereafter referred to as the Archives Regulation)
64. See, Article 6(1) of the Archives Regulation, *ibid.*
65. Recital 6 of 'Proposal for a Council regulation on the security measures applicable to classified information produced or transmitted in connection with European Economic Community or Euratom activities', COM (92) 56 final, submitted by the Commission on 26 February 1992
66. Resolution on the proposal for a Council regulation (EEC) on the security measures applicable to classified information produced or transmitted in connection with EEC or Euratom activities, Official Journal of the European Union, C 176, 1993, at p. 60
67. Bulletin of the European Communities, November 1993, at point 1.7.3
68. The Secretary-General of the Council adopted, for its part, a Council Decision on measures to protect classified information applicable to the General Secretariat of the Council Decision No. 24 of 30 January 1995. These rules have been supplemented by internal rules of the Council and Commission, adopted on the basis of Articles 151(3) and 162(2) EC, on security screening of persons authorised to have access to classified information. See, Council Decision 98/319/EC of 27 April 1998 relating to the procedures whereby officials and employees of the General Secretariat of the Council may be allowed access to classified information held by the Council, Official Journal of the European Union, L 140, 1998, at p. 12 and Commission Decision 99/218/EC of 25 February 1999 relating to the procedures whereby officials and employees of the European Commission may be allowed access to classified information held by the Commission (notified under document number C (1999) 423, Official Journal of the European Union, L 80, 1999, at p. 22
69. 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, at p. 21
70. See, Article 9 of Regulation (EC) 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, *Official Journal of the European Union*, L145, 2001, at p. 43
71. See, Roberts, A., 'Entangling Alliances: NATO's Security Policy and the Entrenchment of State Secrecy', *Cornell International Law Journal*, 26(2), 2003, p. 329-360
72. Recital 15 of Regulation 1049/2001, *op. cit.*
73. See, Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No. 1049/2001 regarding public access to Eu-

- ropean Parliament, Council and Commission documents, COM (2011), <http://www.statewatch.org/news/2011/mar/eu-com-access-reg-1049-proposal.pdf>
74. See, European Parliament resolution of 14 September 2011 on public access to documents (Rule 104(7)) for the years 2009-2010 (2010/2294(INI))
 75. See further, Curtin, D., *Executive Power of the European Union. Law, Practices, and the Living Constitution*. Oxford: Oxford University Press, 2009
 76. Council Decision of 31 March 2011 on the security rules for protecting EU classified information, *Official Journal of the European Union*, L 141, 2011, p. 17-65
 77. See, in particular a series of five declarations entered in the minutes of the Council session at which the Council Decision was formally adopted, <http://www.statewatch.org/news/2011/mar/eu-council-classified-information-8054-add1-11.pdf>
 78. Declaration by the Council and the Commission on the protection and handling of classified information, <http://www.statewatch.org/news/2011/mar/eu-council-classified-information-8054-add1-11.pdf>
 79. 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, *Official Journal of the European Union*, C 202, 2011, p. 13-23
 80. Council Decision 2009/968/JHA of 30 November 2009 adopting the rules on the confidentiality of Europol information, *Official Journal of the European Union*, L 323, 2009, at p. 17 See also, Decision of the Management Board of Europol laying down the rules concerning access to Europol documents, https://www.europol.europa.eu/sites/default/files/public_access_to_europol_documents.pdf
 81. See, Council of the EU, 14031/09, Letter of Europol Director to the Chairman of the Article 36 Committee of 2 October 2009, on file with the author
 82. Council Decision of 6 April 2009 establishing the European Police Office (Europol), *Official Journal of the European Union*, L 121, 2009, at p. 37
 83. *Official Journal of the European Union*, C 190, 2011, at p. 2
 84. See further, in the US, www.archives.gov/cui/
 85. 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', www.fas.org/spp/crs/RL31845.pdf
 86. See also, 'Report of the Commission on Protecting and Reducing Government Secrecy' (hereafter: the Moynihan Committee), Washington: US Government Printing Office, 1997, at p. 29
 87. See, Roberts, 2003, *op. cit.*, at p. 356
 88. Agreement between the European Union and the North Atlantic Treaty Organisation on the Security of Information, *Official Journal of the European Union*, L 080, 2003, p. 36-38
 89. See, Council of the EU, 'Exchange of EUCI with third states and international organisations', 12619/11, 7 July 2011, <http://register.consilium.europa.eu/pdf/en/11/st12/st12619.en11.pdf>
 90. 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

91. See, for example, Article 29(1) of the Regulation No. 3, *op. cit.*
92. See, Article 4(4) and Article 9(3) of Regulation 1049/2001, *op. cit.*
93. See further, Nesson, C.R., 'Aspects of the Executive's Power Over National Security Matters: Secrecy Classifications and Foreign Intelligence Wiretaps', *Indiana Law Journal*, 49, 1973-1974, p. 399-421, at p. 402; see also, Moynihan Committee Report, 1997, at p. 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 believe requires classification, including the use of classification guides.'
94. See, Relyea, H., 'Government Secrecy: Policy Depths and Dimensions', *Government Information Quarterly*, 20(4), 2003, p. 395-418
95. 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 Committee on Government Reform House of Representatives*, 108th Cong., at 82, 24 August 2004, (statement of C.A. Haave, Deputy Secretary of Defence for Counterintelligence and Security); Rumsfeld, D., 'War of the Words', *Wall Street Journal*, 2005, at A12 (acknowledging 'too much material is classified across the federal government as a general rule')
96. B. Franklin, quoted in the Moynihan Committee Report (2007), *op. cit.*, at p. 4
97. See, in general, Thompson, D.F., 'Democratic Secrecy', *Political Science Quarterly*, 114, 1999, p. 181-193; Chenin, M.A., 'Secrecy and Democratic Decision', *Quinnipiac Law Review*, 27(1), 2009, p. 1-53
98. See further, Sagar, R., 'On Combating the Abuse of State Secrecy', *The Journal of Political Philosophy*, 15(4), 2007, p. 404-427, at p. 405
99. Sagar, *ibid.*, at p. 408
100. See further, Sagar, *ibid.*
101. See on US practice, Sagar, *ibid.*
102. See further, in general, Eckes, C., *EU Counter-Terrorist Policies and Fundamental Rights: The Case of Individual Sanctions*. Oxford: Oxford University Press, 2010
103. Case T-284/08, People's Mojahedin Organization of Iran v Council (OMPI III) [2008] ECR II-3487, at para. 73
104. See, European Parliament, 'Study on Parliamentary Oversight of Security and Intelligence Agencies in the European Union', <http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf>
105. Inter-institutional agreements are a long-standing phenomenon in the EC/EU context. See further, Monar, J., 'Interinstitutional agreements: The phenomenon and its new dynamics after Maastricht', *Common Market Law Review*, 31(4), 1994, p. 693-719
106. See further, in general, Beukers, T., *Law, Practice and Convention in the Constitution of the European Union*. Dissertation, 2011, University of Amsterdam
107. See further, Beukers, 2011, *ibid.*
108. Article 9(6) of the Access Regulation. In respect of the Commission the security rules are annexed to its rules of procedure, *Official Journal of the European Union*, L 308/18, 2000, at p. 26 amended several times, consolidated version, see, <http://europa.eu/scadplus/leg/en/lvb/o10004.htm> They do not seem to have been amen-

- ded after the entry into force of the Lisbon Treaty and are no longer annexed to the Commission's new Rules of Procedure, Commission Decision of 24 February 2010 amending its rules of procedure, C (2010) 1200 final, OJ, L 55/60, 2010
109. Article 9(7) of the Access Regulation (2001), *op. cit.*
 110. See further, Rosen G., 'Can you keep a secret? How the European Parliament got access to sensitive documents in the area of security and defence', RECON Working Paper, forthcoming 2012
 111. See further 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, *Official Journal of the European Union*, C 298, 2002, at p. 1
 112. Para. 3.3 of the Inter-institutional Agreement, 2002, *ibid.*
 113. See further, Decision of the European Parliament on the implementation of the Inter-institutional Agreement governing European Parliament access to sensitive Council information in the sphere of security and defence policy, P5 TA, 2002, 0502 and Decision of Secretary General of 21 November 2006 implementing measures for technical questions relating to operation of the Confidential Documents Service and transfer of confidential documents, on file with the author
 114. See the most recent Framework Agreement on Relations between the European Parliament and the Commission of 20 November 2010, OJ L304/47
 115. Annex 11 of Framework Agreement 2010, *ibid.*
 116. See, the 'limited' document 14405/11, Council, 'Draft Interinstitutional agreement between the European Parliament and the Council concerning access by the European Parliament to classified information held by the Council on matters other than those covered by the Interinstitutional Agreement of 20 November 2002', 20 September 2011
 117. See, Article 3(4) of the Draft Interinstitutional Agreement, *ibid.*
 118. Articles 218(6) and (4) TFEU
 119. Article 218(10) TFEU
 120. See for example, Council, 10453.11. 'Draft Agreement between the USA and the EU on the use and transfer of Passenger Name Record data to the US Department of Homeland Security', <http://www.statewatch.org/news/2011/may/eu-usa-pnr-agreement-20-5-11-fin.pdf>. See also, Council of Europe, 'Draft legal instruments on the accession of the European Union to the European Convention on Human Rights', 19 July 2011, <http://www.statewatch.org/news/2011/jul/eu-coe-echr-final.pdf>
 121. See, Sagar, *op. cit.*, at p. 422 et seq
 122. EU-US Negotiations on an Agreement to protect personal information exchanged in the context of fighting crime and terrorism, MEMO/11/203 Brussels, 29 March 2011. See also, Commission, <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/203>
 123. COM (2010) 252/2, <http://www.statewatch.org/news/2010/aug/eu-usa-dp-general-em.pdf>
 124. The Bureau consists of President Buzek and the 14 Vice-Presidents, representing 6 out of 7 political groups in Parliament.
 125. This is explicitly stated by the Council Security Committee in its 'Draft Policy on handling of documents internal to the Council', 7470/11, 8 March 2011

126. Case T-529/09, *Sophie in 't Veld v. Council*, OJ, C 80/32, 27 March 2010, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:080:0032:0032:EN:PDF>
127. Case C-39/05, *Sweden and Turco v. Council*, (2008) ECR I-4723. See also, Case C-506/08, *Sweden v. MyTravel and Commission*, Judgment of 21 July 2011, nyr
128. See, Weber, M., 'Bureaucracy' in H.H. Gerth and C. Wright Mills (eds.), *Essays in Sociology*. Oxford: Oxford University Press, 1946 ('Every bureaucracy seeks to increase the superiority of the professionally informed by keeping their knowledge and intentions secret')
129. See, for example, the President's Office of Legal Counsel legal opinion (at the time secret) authorising torture. By limiting internal circulation of the legal opinion the Bush Administration was able to delay the leaking of its improper conduct and limit internal – and external – criticism, <http://www.acu.org/national-security/memo-regarding-torture-and-military-interrogation-alien-unlawful-combatants-held-o>
130. See, Hood, C. 'From FOI World to WikiLeaks World: A New Chapter in the Transparency Story?', *Governance* 24:4, 2011, p. 635-638
131. See, contra, European Parliament, 'Draft Report on the proposal for a regulation of the European Parliament and of the Council regarding public access to European Parliament', Council and Commission documents (recast), Rapporteur M. Cashman, 1 September 2010, new Article 3a (Amendment 27) which proposes a novel 'procedure for the classification and declassification of documents'
132. See, Thompson, D.F. 'Democratic Secrecy', *Political Science Quarterly*, 114(2), 1999, p. 181-193