Unveiling the Power over Europol’s Secrets

Vigjilenca Abazi

Amsterdam Centre for European Law and Governance

Available for download at www.acelg.uva.nl under the section Publications or at the author’s SSRN page
I would like to thank Professor Deirdre Curtin and Dr. Christina Eckes for valuable comments on an earlier draft. This paper was prepared for the Colloquium ‘Transparency and National Security’ held at University of Copenhagen, Denmark, 4-5 October 2012. The Paper attempts to state the law and factual context as it existed on October 2012.

April 2013

© Vigjilenca Abazi

Address for correspondence
Vigjilenca Abazi
University of Amsterdam
Amsterdam Centre for European Law and Governance
P.O. Box 1030
NL – 1000 BA Amsterdam
The Netherlands
Tel.: +31-20-525-3079
Email: V.Abazi@uva.nl

Information may be quoted provided the source is stated accurately and clearly. Reproduction for own/internal use is permitted.
Abstract
After decades in a culture of secrecy, ever since the Maastricht Treaty the European Union has made efforts to establish transparency as a fundamental principle of European governance. Yet, to what extent is the EU actually transparent? This paper explores new ground by approaching transparency from its flip side. It addresses secrecy and how secrecy operates in practice through the system of classification of documents. Focusing on Europol, an EU law enforcement agency and an important security actor which facilitates Member States to safeguard security through exchange of sensitive information, this paper provides an in-depth inquiry of who is the main actor for classifying documents and what are the implications for such state of affairs. It draws on Europol’s legal framework and enriches the discussion with empirical work by looking at the practice.

Keywords: Europol, secrecy, classification of documents, security, openness.
1. Introduction

There is an intrinsic relation between secrecy and security. Secrecy is both necessary and antithetical to security policies of democratic governance (Note, Harvard Law Review). It is necessary since fighting crime and international terrorism involves sensitive information in need of protection and subject to nondisclosure, which is instrumental to operations, yet antithetical because it keeps information away from the public eye and creates a gap in the civic discussion about most fundamental values in society (Chinen, 2008). Secrecy guards national security by protecting information that would pose an identifiable threat to the security of nation by compromising its defence or the conduct of its foreign relations (Aftergood, 2009, p.402). Further, secrecy is sometimes needed to preserve the element of surprise in government actions (Bok, 1986, p.176). Instances of these justifications include the need for secrecy in the development or abandonment of plans and missions in wartime but also of law enforcement actions such as conducting an arrest. In this sense, there is tolerance for secrecy in a democracy when it protects various types of genuine national security information, from advanced military technologies to sensitive intelligence sources, from confidential diplomatic initiatives to fighting serious crime. When properly employed, secrecy serves the public interest (Aftergood, 2008, p.103). Yet, it seems that with many issues falling in national security, people “cannot evaluate some policies and processes because the act of evaluating defeats the policy or undermines the process” in question (Thompson, 1999, p.182). In order to remedy this situation citizens must be able to know how secrecy is used in a democracy and who retains the power over it (Kitrosser, 2007).

Classification of documents is the predominant manner in which secrecy appears in practice (Hall, 2005). Technical at first sight, rules on classification actually mirror the structure of power and control within an organization (Curtin, 2003). Classification of documents reflects a deliberate act to withhold information with the aim to protect it from unauthorized access. Therefore, blocking information and doing so intentionally is the starting point of secrecy. The classification system sets apart the secret keepers, those that classify and have access to classified information, and those outside the secret circle. Being a convenient tool by which the insiders can keep
interference away from outsiders and if necessary hide embarrassment, secrecy through classification of documents is efficient for maintaining and enhancing power (Webber, 1946). Furthermore, within the production of secrecy there is “always a problematic concern of participants because some are much more successful than others at practicing in it” (Bellman, 1981, p.1).

How do these dynamics of secrecy materialize in the European Union (EU)? After decades in a culture of secrecy, ever since the Maastricht Treaty the European Union has made efforts to establish transparency as a fundamental principle of European governance (Birkinshaw, 2010). Yet, at the same pace rules on classification of documents and other ‘secrecy’ measures are much more far reaching in terms of scope and width as the latest rules of the Council in March 2011 illustrate by incorporating all EU bodies in its “secrecy web” and applying to a broad spectrum of all its activities (Curtin, 2011, Council Decision, 2011). The mechanism of classification hides information away from the public eye and compiles a large body of secret information for reasons of, inter alia, public security and international relations. Of all refusals for access to documents, 95% fall under these two exceptions (Tenth annual report of the Council on the implementation of Regulation No. 1049/2001). This effectively makes the classification system a trump card for keeping secrets in the EU in the name of security.

Thus, questions arise, who determines what becomes a secret and how it is kept? Answering these questions is salient not merely for understanding the power structure behind the scene of secrecy but it is also telling on how actors in the EU manage their daily tasks while being under the general obligation of openness in the EU as stipulated by Article 10, Treaty on European Union. Additionally, the relation of secrecy and security brings the actors a situation of tension between protection of documents through classification on the one side and the need for operational flexibility where information can be easily exchanged on the other side. In achieving the right balance between these pulling forces, an EU actor must have sufficient power in deciding what gets classified, at which level and for how long. Moreover, in order to avoid information asymmetry and overclassification, an actor must be in charge for the major decisions involved in the classification process such as access, protection, and its exchange (Goitein, 2011, Stiglitz, 1999). With other words, both
the democratic imperative and the operational flexibility require a balance between secrecy and openness as well as protection of information and successful application of security measures. Balancing here is understood not in a static and abstract sense but rather a practical plan for achieving these goals. Review of classification, for instance, is a concrete tool for realizing this dynamic balance and often the key to a successful system (Doyle, 1994).

This paper examines who retains the power over classification of documents by analyzing one specific EU actor: Europol. Namely, Europol is a law enforcement agency and important in security matters dealing with more than 10,000 cases a year in order to support Member States in enforcement operations (Europol, 2011). In 2009 the Council adopted the Decision establishing Europol as an EU agency making management of information and its exchange Europol’s raison d’être (Europol Decision, 2009). Along with its establishment, the Council provided Europol with the main tool for its work: the system of classification of information. Nowadays, Europol’s activities in security expand from fight of serious crime, drug trafficking and terrorism to the more recent policies of cybercrime and cyber security (O’Neill, 2012, Argomaniz and Carrapico, 2012). Apart from developing a prominent role in security substantively, Europol has also advanced in its manners of keeping secrets from a system characterized by an ad hoc approach to a sophisticated secrecy mechanism (Interview E1). But do these developments result in Europol having a dominant voice when it comes to classified information, and hence be held accountable for its decisions, or is Europol merely a “clearing house for information” facilitating “27 different cultures of secrecy with some Member States having a tendency to overclassify” (Groenleer, 2009, Interview E4)?

The paper explores new ground by drawing on Europol’s legal structure and enriching the discussion with empirical work through interviews with former and current practitioners. In doing so, the analytical framework of ‘life-cycle information’ is applied (Bruk, 1988, DeSanti, 1993, Hernon, 1994). This framework offers a holistic perspective of classified information by examining information throughout a life span in which decisions must be made with respect to creation, management and final status. The life-cycle approach provides a meaningful insight in assessing the initial decision to classify throughout the period in which the
information is of value (Moynihan, 1997). Three particular elements – initiation of classification, access and exchange of classified information – of the lifecycle framework are discussed here in order to decipher who is the main actor for classification. These elements are the gist of the system, hence the decision-making power is mostly relevant at these stages.

In light of the aforementioned, the paper sets out the legislative matrix and the actors involved in classification (part two) and focuses on the commencement of classification by asking who actually makes the initial decision to classify a document (part three). The elaboration on the main actor is continued by zooming inside the secrecy game and asking who controls access and exchange of secrets (part four). Against this background, review of classification is discussed in order to point out the implications of the current arrangements both for openness and security (part five).

2. Classification in Europol: what are the rules and who are the actors?

Emile Durkheim argued that removing something from the public review endows it with power and the object of secrecy – its information – is often less important than the organizational approach to managing it (Durkheim, 1915). In that sense, the following section focuses on rules by which information is removed from public’s eye and on the actors involved in this process.

2.1 Regulated secrecy

Regulated secrecy is composed of the norms and practices of classified information through which efforts are devoted to manage sensitive information. It is secrecy since the information is publically undisclosed and it is regulated considering it is arranged through decisions or other legal instruments. Secrecy is most commonly regulated through executive’s sole competence without involving people’s representative. However, arguments have been raised that the basic rules governing classification and declassification should be the product of an open discussion that weighs both the advantages and disadvantages of secrecy and that is not restricted to
the views of those charged with implementing regulations (Report of the Commission on Protecting and Reducing Government Secrecy, 1997). In practice, nevertheless, executive orders – such as in the USA since 1951, or internal rules of procedure – such as in the EU since 1958, are the means through which secrecy is regulated. In this respect, Europol follows the tradition.

Europol, unlike many other international police cooperation networks or bodies, was not formed bottom-up by police professionals but is a result of a top-down decision by political and legislative bodies in the EU (Deflem, 2006). Since the Amsterdam Treaty there have been attempts to build a legal and institutional framework in order for Europol to be fully operational for fighting cross-border crime (Busuioc, 2011). In 2009, the Council established Europol as a law enforcement agency bringing it within the EU umbrella where the European Parliament (EP) could also play a role such as in the adoption of the budget (Council Europol Decision, 2009). Along with its establishment came the need for a robust security information management considering that sensitive information collection, analysis and exchange are Europol’s core tasks. In that sense, there are two Decisions by the Council that form the core rules and principles in a general manner for Europol classified information, i.e. the Council Decision on the confidentiality of Europol information (Europol Confidentiality Decision, 2009) and the Council Decision on rules governing Europol’s relations with partners (Information Exchange Decision, 2009). Both Decisions establish a concrete modus and rules by which Europol handles classified information, leaving the more specific details, however, to the Security Manual adopted by Europol’s Management Board.

Protection of information is a high priority for Europol. Consequently, basic protection is given to all information processed by or through Europol. Namely, the Europol Confidentiality Decision establishes a categorization of information since Europol deals with many types of information coming from various sources. In order to best manage, utilize and protect information, Article 10 (1) divides information in three major categories: public information, basic protection information, and classified information. Due to its nature, being a law enforcement agency, Europol in this regard differs from other institutions in the sense that unless the information is intentionally and expressly marked as public it remains undisclosed, either under
basic protection or under the classification regime. Hence, in Europol there is a presumption for secrecy which in practical terms means “secret (protected) unless…” Europol’s public information can be its newsletter or official reports aiming at increasing public confidence in its activities. Interestingly, the EP is also treated as the general public, which means that the EP is only given access to information that is not under basic protection or classified. According to one official the rationale for not sharing classified information with the EP is that they “could have a problem with the Member States actually asking “if Europol starts releasing - information to the EP will it happen maybe at some stage that someone in the EP will come up with a classified information that we classified in the first place and will they start showing it to the public or the internet, that can easily happen…” (Interview E2) This situation would be highly undesirable for Europol since they “can only live on the information that [they] receive …from the Member States” (Interview E2).

Further comprehensive measures on protecting information are laid down in the Security Manual. This detailed legal act is not accessible to the public since, to put it in the words of Europol’s official: “people could actually see how we protect information and we do not want that” (Interview E4). A Management’s Board Decision on public access to Europol’s documents regulates the other side of the coin, i.e. openness. This Decision acknowledges the importance of openness as a guarantor of greater legitimacy. Yet, in Article 5 it confirms that the originator principle is applicable. Namely, under the originator rule, the actor that provides information (actor A) retains complete control over its dissemination by the actor which receives it (actor B). If the information has been classified by actor A, it cannot be reclassified or declassified by actor B, unless actor A consents to the change. Similarly, no information provided by actor A can be given by actor B to a third party -- such as another government, organization or citizen - without the consent of the originator. Actor A’s control over shared information is absolute. There are no norms or review mechanisms that oblige actor A to justify its decision to refuse a request for declassification or release of information which it has provided to actor B (Roberts, 2008). In order to ensure the originator rule along with other security requisites, internally the security unit establishes the so-called security policies and security operating procedures. These procedures concern issues of classification such as the manners of distribution of classified information, its reproduction or its destruction.
Security operating procedures are thorough – they concern very technical matters related to physical protection of the information.

The regulation of secrecy, however, is merely an initial step to ensure functionality of the system. The actors involved are “the linchpin of classification” (Report of the Commission on Protecting and Reducing Government Secrecy, 1997).

2.2 The Actors Involved: Classifiers

In general, there are two types of actors involved in the classification system: the ones that hold the initial classifying authority, and the rest that classify because they have in some way used information from a classified document (Quist, 2002). Original classifiers are actors with higher classifying authority permitted to classify information in the first instance. Typically department or agency heads, or other senior officials are designated in this task. Derivative classifiers are actors who, while working with classified information, generate or create new documents and materials based upon them. Derivative classifiers who reproduce, extract, or summarize classified information, or who apply classification markings derived from source material or as directed by a classification guide, do not need to possess original classification authority. They are obliged to classify the newly made document based upon the classification level of the information from which the new document was developed.

Europol to a large extent is in a position of a derivative classifier. An acknowledgment from a practitioner is an explicit illustration of this phenomenon (Interview E2):

“…I would say that 95 % of the information that we have here that gets classified is not classified based on our own decision but it is classified by the decision of the originator…we are talking about…perhaps 10-20 documents per year that are classified just by Europol. I am saying we have high level of classified documents but that is …from the documents we create based on those documents always based on the original classification.”
Hence, the relation between the Member States and Europol in the majority of cases is that of original classifier and a derivative classifier. But the dominant presence of the Member States is not only numerical, they are also present in Europol’s structures. To start with, there is the Security Committee, in charge to set the broader policies, which is comprised of representatives from the Member States. To implement the policies set, coordinate and control all matters that fall within the security of classified information, one of the three deputy directors that assist the Director of Europol is assigned. This official, called the Security Coordinator, monitors the enforcement of security provisions and makes sure that no breaches occur.

The day-to-day work within Europol is done by the security officers who are assigned specific tasks to instruct, assist and advise all persons at Europol regarding security of classified documents. “Confidentiality desk official” is the official job title of classified information experts who deal with facilitating the access, production, reproduction and other matters concerning classified information in Europol (Interview E1). In addition, they enforce security provisions, investigate breaches and report them to the Security Coordinator. The security clearance of these officers depends on the level of their function within Europol. The regulations of their national state are also taken into account. The confidentiality desk officers can guide the head of unit if the level of classification or any other matter concerning classification is not clear. The key figures when it comes to classified information within Europol are the head of units, with them lays the main responsibility, they are the owner of information within Europol. In this sense, another distinction to be drawn in terms of actors is between the originator of the information and the owner of the information, which are not in all cases the same person. Depending if the information is actually produced by Europol or not, Europol can be both the originator and the owner or only the latter. The notion of ownership is there to facilitate the process of tracing responsibility within one particular organization for classified information when it comes to its protection, level of classification, access to information and so on. In cases where the Member States, for example, share information with Europol, upon receiving that information a head of Unit is assigned as the owner of the information for the purposes of Europol. What this implies is that the person designated as the owner has the overall responsibility over that information within Europol’s operation. Thus, the originator is the Member State that
is sending that information and they retain all the privileges that come from having such a position due to the originator principle. In the case where Europol is producing information that is classified then it is the person issuing that document that is both the originator and the owner of the information within Europol.

In sum, Europol’s classification system is regulated mainly by the Council although specific and technical matters are managed by its security unit. More importantly, Europol to a large extent is a derivative classifier. This implies that most of the fundamental decisions regarding secrecy are not made by Europol. The following sections will discuss if indeed that is the case.

3. The main decision-maker in the initiation of the classification process

The initial classification determination, establishing what should not be disclosed and the level of protection required, is probably the most important single factor in the security of all classified programs (Thompson, 1969). None of the expensive personnel-clearance and information-control provisions (physical security aspects) of an information security system come into effect until information has been classified. The first decision is the pivot on which the whole subsequent security system turns (Moynihan, 1997). Therefore, it is important to classify only information that truly warrants protection in the interest of security. However, the task of deciding which information is to be classified, at which level, and for how long remains in large part a subjective judgment open to a range of interpretation. Officials admit that there is no such thing as a mathematical formula which gives all the answers. Consequently, the individuals who classify information should be made aware about the implications of their decisions (Interview E4).

There are three main and most important decisions at the very outset of classifying: first, determining whether a document should be classified; second, establishing its classification level; and third, indicating its duration of classification. Thus, the first stage of classification identifies the information that must be protected against unauthorized disclosure. Security measures thereafter determine how to protect information which has been classified (Church, 1966).
At the start of the classification process, i.e. making decisions if information should be classified, the position of an original classifier and derivative classifier does not differ much. The derivative classifier also makes a similar decision with respect to documents by asking whether the document should be classified because of the information it contains or reveals. What is meant here is that the base of a document being a classified document in itself does not require absolutely that the other document is also classified. Rather, if the information from the classified document is contained in the newly made document then the deriving document is classified at the same level as the original one. Mention here should immediately be made to the concept of “born classified” (Green, 1981). This concept assumes that newly discovered information might be so significant with respect to security that it requires immediate and absolute control. The main characteristic of this concept is that positive action is not required to put information in this category because if information falls within the definition of the legal act it is in this category from the moment of its origination (hence the name “born classified”). A unique example of this concept is to be found in the USA, The Atomic Energy Act of 1945 where there is an assumption that the newly discovered atomic-energy information is important for security reasons and it requires instant and utter control (Hewlett, 1982, Quist, 2002). This concept is not known in Europol.

In Europol’s practice, but also more generally, the life of a classified document starts at the early stages of drafting. As a practitioner explains (Interview E1):

“Who makes the decision most of the time? The drafter. He has a certain view and expertise on the subject matter, a certain understanding or interpretation of the rule, he may want to use classification to give importance to his work, may need to respect the confidentiality level of the information he used, or following his national background, classifies certain issues a certain way – or classifies everything. Classification is subjective – it is a judgment call.”

However, most of the time the drafting process actually starts at the national level. Europol is wholly reliant on information received from Member States (Brady, 2008). Member States’ position in regard to the initial step of classification matters particularly in two instances. Firstly, when the Member State supply already classified information to Europol they are responsible for the choice if the
information should have been classified, at which level and for how long. A classification level indicates the relative importance of classified information to security and thereby determines the specific security requirements applicable to that information. Clearly defined classification levels are essential to an effective classification system. The appropriate classification level would be expected to usually be determined by the information disclosure risks because those risks largely determine the magnitude of the harm that could be caused by such disclosure (Quist, 2002). In choosing the classification level, Member States take into account the classification of the information under their national regulations. Europol Confidentiality Decision does mention that Europol’s need for operational flexibility should be taken into account, but in practice that would mean that a national police officer should know what level of operational flexibility Europol needs for a certain investigation and take this into serious account before classifying information. Yet, as recent empirical work has shown “most police officers still think and act nationally or locally” (Busuioc, 2011).

Operational flexibility is very important for Europol to deliver successful results and it is conditioned by having information which is protected at the appropriate level (Interview E3). If the level of classification is higher than restricted for Europol it creates not merely a more burdensome administrative procedure but also goes against the logic of being operational and finalizing the case in national courts where adjudications require information to be shared with the defendant or the general public. In case Europol comes to the conclusion that the choice of a classification level needs changing (for instance removing or adding a classification level, or adding a classification level to a document previously subject to the basic protection level), it cannot undertake any action without a prior agreement of the Member State providing the information. Although Europol itself might be “reasonable” when it comes to the level of classification, due to “27 different approaches from the Member States” with some having a tendency to over classify, it ends up being bound by the culture of classification of the Member States (Interview E4).

It is not merely the level of classification that can be disputed there might be a similar case with its duration. Classification duration may be defined (1) in terms of a time period measured from the origination date of a document (i.e., at a future date) or (2)
in terms of a future event which must occur prior to declassification. Therefore, for classification decisions, the question is whether duration of classification can be specified for classified information or whether no duration can be specified so that declassification must await the actual disclosure event. In practice, Europol officials acknowledge that they need operational flexibility and that they are bound by the “spirit of the legislator [that is] not [to] create secrecy” (Interview E4). In order to achieve these goals, classification duration in principle is kept for five years.

The second instance when the position of the Member States is significant involves situations where information is generated by Europol, however based upon, or contains, information supplied by a Member State. In this case Europol determines the level of classification, but again this is done in agreement with the Member State concerned. It is only when Europol itself generates information, and such information is not based upon, nor contains, information supplied by a Member State, that Europol itself determines the appropriate classification level. However, the latter case is less frequent and is based on information that come from open sources and private sources. It is only a recent trend that police cooperation widens to include forms of actors in which the private sector is seen as a partner (Dorn, 2009). However, practically this category of information remains very small in number. Thus, when it comes to the decision if information should be classified and all the consequences that follow, Member States most often than not make the final decision. This position has implications not merely for determining if a document becomes part of the classification regime but also for the “life” of that document henceforth. Europol may advice a Member State that a classification decision should be reconsidered, yet in practice this has hardly happened, partly due to Europol’s need for information. In addition, the initiation of classification brings with it the culture of classifying of Member States which indirectly becomes “binding” for Europol. Historically, there are different approaches from the Member States - some do over classify. A difference in classification culture is particularly evident after 2004 – it takes time before Member States draft with an EU perspective (Interview E4). Is the situation different once a document is classified and is in Europol’s ownership? With other words, does Europol gain a voice?
4. Dynamics inside the secrecy game

The classification system ensures that access and exchange of information is only granted to authorized individuals. Consequently, all the mechanisms build in the system are focused at these two key points. Who allows access and/or exchange of classified information in Europol?

4.1 Controlling Access to Secrets

The most important aim of protecting documents is to avoid unauthorized access. Hence, within the classification system access is considered as a central element for protecting sensitive information. Apart from the positive effect of protecting information, access can also be a tool to determine who is part of the “insiders club of information” and who is not. Echoing Bok, secrecy presupposes separation, a setting apart of keepers of a secret from those excluded (Bok, 1986). Hence, determining who has access is a practical reflection of the authority to determine the insiders and outsiders of secrecy. Within the system of classifying information there are two principles, usually in interaction, which determine access to classified information: the need-to-know principle and the level of classification of the information. The need-to-know principle is one of the conditions that the individuals within the organization need to fulfil in order to gain access to the classified information. As the wording implies, access is granted if there is a need, either due to obligations or position, for the individual to acquire that information. Additionally, the level of classification determines who would access the information considering that higher levels of classification are reserved for higher level of officials within the administration. These two aspects of the classification system provide a useful kit when it comes to ensuring the security and protection of the information, however at the same time they also enable that the information is compartmentalized. Such phenomenon impacts the decision-making process both in terms of efficiency and creating a cluster of inside-insiders, i.e. only a limited number of individuals knowing the classified information. In this light, firstly, secrecy provides the opportunity for special interest to have a greater sway (Stiglitz, 1999); secondly, it creates a situation where decisions are made with imperfect information and may lead to not achieving optimal results that might have occurred if more had been
known (Scheppele, 1988). Apart from the need-to-know principle, security clearance is also necessary in order to gain access to classified information. Security clearance implies that a vetting procedure takes place in order to determine the loyalty, trustworthiness and reliability of a person concerned.

In sum, in order to access information, an official must have a security clearance and a need-to-know for the information. In Europol, these conditions are governed by Member States’ consent, decision, and action. Namely, where Europol intends to entrust persons with a sensitive activity, at the request of the Director of Europol, Member States have the responsibility to arrange the security screening of their nationals. This is done in accordance with the national provisions and the results are binding on Europol. There is also an obligation to provide assistance to each other with the security screening considering particularly that only persons that have undergone the special training and screening are allowed access to classified information. Hence, all persons who have access to information subject to a classification level must have a security clearance which is issued by the Member State. They might have different principles but “everyone has the same minimum standards” (Interview E4). There are some states that have more rigid procedures, for example they check more personal data for the individual concerned for a longer period of time or have a lie-detector which might not be allowed in other countries. Nevertheless, the procedure of security clearance is under the authority of the Member States.

Not all Member States have the same speed of issuing the security clearance and in order to remedy a situation where an individual starts working in Europol but lacks a security clearance to actually access information, a temporary security clearance is issued (Interview E2). The temporary authorization can last up to a maximum of six months, however information granted under this authorization cannot be at the security level of “SECRET EU/ EU SECRET” or beyond. Thus, it is a mechanism to enable persons to get acquainted with the classified information in order to fulfill their obligations. However, since the security clearance is not yet granted there are three cumulative conditions under which this authorization may be given: first, it is in the interest of Europol for the person to know the information; second, the national authorities have been given a notification; third, the national authorities
have no reaction within three months. After the authorization is given, the security coordinator informs the national authorities. Lastly, when a Member State provides information to Europol it can specify that the temporary authorization cannot be exercised in relation to that information. When it comes to persons cleared at national level, it is the security coordinator who grants authorization for access. Again, the principle of need-to-know on the basis of the duty or obligation is applicable. This authorization, however, is subject to regular review by the security coordinator and can be withdrawn on justifiable grounds. Security screening is subject to annual check for which the Director prepares a Report submitted to the Management Board. Granting a security clearance for a certain level of classified information is not supposed to mean that an individual gains access to all information classified at that level. The dissemination of classified information is intended to be limited to those who both (1) hold the appropriate clearance, and (2) need the information in order to properly perform their duties.

While the security clearance can be seen as something more permanent, subject to reviews at times, the need-to-know condition is dynamic in the sense that it can differ depending on official’s position and specific subject of work. Within Europol, it is the owner of the information that decides who has a need to be acquainted with the information. For instance, “if…someone [is] working on cocaine trafficking in principle he should not have access to information that [other officials] have when it comes to human trafficking. Unless, for instance a suspect dealing with cocaine is also mentioned in human trafficking, of course some of these organizations deal with multiple form of crimes…[that official then] can access [the information]. But only if there is a need to know – so you have need to know and nice to know. It is only if you have need to know that you access it” (Interview E3).

The Member States can be explicit about who can get access to their information within Europol and beyond through the so-called “handling codes”. Namely, a handling code (as the name suggests) determines how the information will be dealt with in judicial proceedings and how it will be shared with the rest of Member States. There is an imperative that the information must be handled in accordance with the wishes of its originator. There are different handling codes as a practitioner explains (Interview E3):
“What we have at Europol is handling codes H1, H2, H3, so every time a Member State sends information to us – if they put H1 on it means this can be shared with all Member States, unless they want to use in in judicial proceedings we have to ask our adviser our authorization again. H2 means that in principle means that it cannot disseminated with anyone – you send it to Europol but you cannot send it to any other Member State. So every time Germany sends us something with H2 and we think to share it with Finland we go back to the Germans asking if they agree that we also share with Finland and they decide. H3 basically means any other restriction – so if the Member States wants the document is accessed only by a certain group of people or even certain individuals they will have to put it as H3 saying this can only be seen by the director and work file X.”

The elaboration thus far implies rigidity of the system which is correct when it comes to information classified from Confidential and higher. But, every individual at Europol, almost except for some contractors or legal inters, has access to restricted information which is also the highest number of information (Interview E2). That makes 800 people (Interview E1, E4, Europol official web page). This number is impressive especially considering that restricted information can contain very sensitive issues among which operational plans for EU police investigations or updates on security risks at foreign embassies, to name but a few examples.

Against this background, the question arises, if access to secrecy is provided for so many individuals, how is exchange of secrecy organized?

4.2 Secret sharing

Exchange of information is the core of Europol’s activities. This implies that the system is comprehensive and complex. Europol exchanges information with the Member States, the European Union bodies and third parties. Out of these three relations, the exchange with the Member States is most developed and important. Notably, Europol exists in order to facilitate the Member States’ direct fight against crime (Bruggeman, 2007). Nevertheless, the relation with EU bodies and third parties
is also relevant especially since Europol aims to have a broad and coordinated approach to information coming from all parts of the world in order to provide reliable reports on threats assessments.

In order to capture the main decision maker when it comes to exchange of information, this section analysis Europol’s exchange of information firstly with the Member States, secondly with a EU body, and lastly with a third party. This provides a full picture for different instances where Europol appears as an information broker.

**Sharing with Member States**

Europol relies predominantly on the Member States when it comes to information on serious crimes (Report House of Lords, 2008). Europol may of course directly retrieve and process data from publicly available open sources such as media and public data and commercial intelligence providers. Nevertheless, without the intelligence sources of the Member States, Europol would not be able to fulfil its mandate (BBC Monitoring Europe, 2001, Kirk, 2001). The Member States play a double role in providing Europol with information. They provide Europol with raw data that Europol incorporates in its system of information management. The raw data collected is then evaluated and analysed by Europol. In this case it is Europol that classifies the later developed information. This type of information is also known as information generated by Europol based upon, or containing information supplied by a Member State. However, the Member State also provide Europol with already classified information that Europol is only left to protect and use. In this context, the exchange in the stricter meaning of the term takes place considering that Europol likewise provides the Member States with classified information. The exchange between the Member States and Europol happens through the liaison officers who assist in particular by providing Europol with information from the seconding national unit and co-operating with the officials of Europol by providing information and giving advice as regards analysis of the information concerning the seconding member state (third party liaison officers have in principle the same tasks and facilities as the member state liaison officers, with the exception of access to the Europol computer systems).
The Europol national unit is the only liaison body between Europol and the member states; all information is exchanged through this unit. The national units have access to relevant national data and to the Information System of Europol. The system allows the rapid reference of the information available to the Member States and Europol. Member States are be able to input data directly into the system in compliance with their national procedures, and Europol can directly input data supplied by non EU Member States and third bodies.

As was noted, when a Member State supplies Europol with classified information it remains the sole authority to determine the classification level, the change of this level and its declassification. Moreover, the classified information is under the responsibility of the Member State which means that decisions regarding access to this information, such as authorization or security clearance, are taken by national authorities.¹ There is, however, a caveat when it comes to the exchange of information between Europol and the Member States. It has been reported that with every Member State having a number of liaison officers located within the same building in Europol it is inevitable that some exchanges of information take place informally between liaison officers without involving Europol at all, even though dealing with matters within its competence. The UK House of Lords reported on this matter with the call for improvement (Report, 2008, para. 50):

“We were astonished to read in the Home Office written evidence …that the vast majority of information exchanges between liaison bureaux occurs outside the formal systems, and thus while providing very significant benefit to the participating countries the main loser is Europol, which is denied the opportunity to access the information. It is reported that up to 80% of bilateral engagement occurs this way…”

Europol’s added value lays in its analysis and report which are a result of assembling classified information from the various sources they receive. If an analysis is of a general nature and of a strategic type, the report is shared with all Member States. But if an analysis bears on specific cases not concerning all Member States and has a direct operational aim, the only Member States that can access the report are those that provided the initial information leading to the opening of the file, those which are directly concerned by that information, and others that these Member States

¹ Article 10, 11, 12 13, Europol Confidentiality Decision
might invite to participate. Other states may learn about the existence of the analysis file through a computerized index and may request to be involved in the exchange but the originator State may object, hence prevent, others to have the information.

As in other matters, exchange of information is dominated by one particular theme that of the originator rule. This seen in combination with the fact that the Member States are the biggest provider of information means that both directly and indirectly they dominate. Yet, some Member States still do not give Europol sufficient or consistent support (Brady, 2008). Some have explained this phenomenon in terms that sharing information, albeit the core of Europol’s work, is problematic because “the national agencies fear that sensitive information might be leaked” (Wille, 2008, p.57). Europol remains “an intergovernmental dish with some communitarian sauce” where Member States may or may not share information. And if they do share, they do it on their own terms.

Sharing within

The Council has established a particular decision that deals with which third parties Europol can exchange information and how this should be done, i.e. Information Exchange Decision. But within the EU legal matrix, on the basis of primary law, Europol may establish and maintain cooperative relations with the institutions, bodies, offices and agencies of the European Union. For Europol’s work information exchange with other actors is necessary and significant.

The exchange of classified information between Europol and a EU body is permissible only in so far as agreement on confidentiality exists between them. This confidentiality agreement is part of the cooperation agreement Europol would have with that body. However, before the entry into force of an agreement or working arrangement with an EU body, Europol may directly receive and use classified information in so far as it is necessary for the performance of its tasks. When it comes to transmission of classified information, however, it is very interesting to note that in Europol’s relations there is a difference between relations with EU’s bodies and the relation with third states or organizations. The difference is that when it comes to the Union, Europol must have an agreement with that particular body in order to exchange classified information, this means that before the agreement enters

\[\text{Article 8, Information Exchange Decision}\]
into force there can be no exchange of classified information. While as when it comes to third parties Europol can exchange information even before the agreement enters into force.³ Lastly, in exceptional cases there can be transmission of classified information to third parties which Europol holds. In this case, the Director of Europol, who might consider this transmission to be absolutely necessary to safeguard the essential interests of Member States or of Europol, decides and informs the Management Board and the Security Committee.

Europol has established interactions with many bodies of the European Union. For instance, Europol cooperates with Eurojust ever since they concluded a first operational agreement in 2004, which was revised in 2009 (Agreement, 2009). The main purpose of this agreement is to make the investigation and prosecution of crimes within the agencies’ respective mandates as efficient as possible and to avoid duplication of effort wherever possible. This agreement provides for the exchange of operational, strategic or technical information, and personal data. In 2008, a secure communication link was established to facilitate the exchange of information between Europol and Eurojust and they have agreed on a table of equivalence to exchange classified information above the level of ‘restricted’. In this exchange, both parties are bound by the originator rule which indirectly makes the Member States involved. In addition to information sharing, a staff exchange programme between Europol and Eurojust started in 2011. Europol and Eurojust write joint press releases and joint documents, for instance, on judicial-police cooperation in operational cases for the EU’s Standing Committee on cooperation on internal security. With regard to information exchange between Eurojust and Europol information may be transmitted either spontaneously or on motivated request⁴ whereby a specification of security and classification of information is included in the Memorandum of Understanding (Serzysko, 2011).

Sharing with the outside

The other two sources of information exchange are third states and international organisations. In the past years there has been an increase of information exchange which occurred through the Secure Information Exchange Network Application. Yet,

³ Article 10, 11, 9, 12, Information Exchange Decision
⁴ Article 8, Agreement between Europol and Eurojust
even if there is a cooperation agreement it does not necessarily mean that there is a proper table of equivalents. Therefore, a confidentiality agreement is also negotiated apart from the parties being involved in the form of cooperation agreement.

Europol can establish either a *strategic agreement* or an *operational agreement* with a third party. Strategic agreements enable Europol to establish a general framework of cooperation to be actually implemented on a case-by-case approach by request of one of the parties, while as operational agreements suggest a constant approach. Additionally, the difference between a strategic agreement and operational agreement is that the first excludes the exchange of personal data while as the second does not. Among many others, Europol currently has operational agreements with Interpol, Australia, Canada, Croatia, and the United States, including a ‘supplemental agreement’ on exchange of personal data with the US while as it has strategic agreements with Albania, Colombia, Russia, and Turkey, as well as with the United Nations Office on Drugs and Crime (UNODC) and the World Customs Organisation.

Both types of agreements concern the exchange of classified information which is done via a designated contact point. The same principles and responsibilities applicable to the member states’ Europol national units apply equally to the units designated in each of the third parties as the point of contact with Europol for the exchange of information within the frame of the co-operation agreement. These units are called National Contact Points (NCPs) and they operate as a Europol national unit except they have no access to the Information System of Europol.

The case of information exchange with the USA provides an interesting example of exchange of information with third party and the role of the Member States in this interaction. The USA and Europol signed an agreement in 2001 and one in 2002 which allows the USA law enforcement authorities and Europol to share both strategic information (threat tips, crime patterns, and risk assessments) as well as personal information (such as names, addresses, and criminal records). Europol and the USA aim to implement common standards on clearances and to develop adequate measures for the exchange of classified information. Best practices are
shared already and exchange programmes for analysts take place on a regular basis in strategic and joint operational actions (Archick, 2012).

However, the relation with this partner is not always amicable. Despite growing USA-EU ties and agreements in the law enforcement area, some USA critics continue to doubt the utility of collaborating with EU-wide bodies given good existing bilateral relations between the FBI and CIA (among other agencies) and national police and intelligence services in EU member states. Many note that Europol lacks enforcement capabilities, and that its effectiveness to assess and analyse terrorist threats and other criminal activity largely depends on the willingness of national services to provide it with information. Meanwhile, European officials complain that the United States expects intelligence from others, but does not readily share its own (Archick, 2012).

The overview of exchange of information leads to three particular conclusions. Firstly, Europol is dependent on Member States’ will to provide it with information and Europol is obliged by that will when it shares information with other partners. Secondly, Europol’s cooperation within the EU legal contours is determined by primary law and the presence of Member States in this type of exchange is manifested through the originator principle. Thirdly, Europol has established many contractual relations with third parties. Yet, some of them including key security players prefer to share classified information with the Member States directly bypassing the sophisticated secrecy mechanism of Europol.

5. What are the implications?

It has been noted on several occasions that national investigative, prosecutorial, and judicial authorities remain the key actors in European law enforcement (Busuioc, 2011) and that Europol is still not playing a central role in European police cooperation (Report House of Lords, 2005, 2008). Perhaps this should not be very surprising considering that by law Europol’s mandate is to support Member States (Europol Decision, 2009). Some see this as “design flaw” considering that no real responsibilities are transferred (Wille, 2008). But the concern for the present purposes is not focused on transfer of competences per se. The question here is what the implications for such a status mean for classification of documents in Europol and
what the consequences are both for the democratic imperative – the requirement of openness stipulated by primary law, and operational flexibility – exchange of information and successful law enforcement operations. As it was elaborated in more detail above, Member States retain the authority to decide what happens with the secrets they create. How these secrets are created, who grants access to them, and other relevant actions in the classification process, are all decisions that Member States make. Is there a significance that the Member States are so central to the classification system of Europol or is this situation unproblematic since it is their secrets after all?

Although throughout the 1980s the idea of a European-style FBI was put forward (Bunyan, 1995), Europol has always performed facilitator-like functions and not executive competency (Bruggeman, 2007). *De facto* Europol could have increased its role to a more autonomous agency especially after its entitlement to ask Member States to start an investigation, yet it has remained limited. Some have explained this limitation by the lack of trust of Member States towards Europol (Walsh, 2006, Kaunert, 2010). A further explanation based on mistrust suggests that national agencies that do not have reservations about sharing information with Europol, remain cautious because of the effect this may have on their “well-established and successful bi-lateral relationship with other, more apprehensive states, most notably, but not only, the USA” (Cross, 2011, Walsh, 2006). Others insist, in general, those who are responsible for maintenance of security systems do not need to know anything about the secrets they protect (Coser, 1963, Lowry, 1972) hence their autonomy is irrelevant in order to safeguard security. In sum, the general literature on EU intelligence tends to focus on the normative (trust) or functional (efficiency) incentives member states need to have toward cooperation (Cross, 2011).

Europol seems to be of the idea that trust comes first and foremost, especially considering that there is no legal obligation for the Member States to provide it with information. An experienced official explains (Interview E2):

“We need to maintain high level of trust... that we can actually protect their information. We can deal with it in the way they want us to. If we start making some sorts of decisions on our own or play any kind of game with the information that we receive of course there is the danger always
that they will just stop giving us the information because there is no legal
obligation for the member states to actually provide us with the
information it is up to them what they provide to us... if they just decide
that [we] are not trustworthy enough to actually release the information
then they can just use the system of the liaison bureau to work again on a
bilateral bases. We can just be not in the picture.”

The Member States play a double role in the classification system of Europol. One the
one hand, they provide most of the information which Europol analysis. On the other
hand, they are the receiver of the end product – the reports encompassing classified
information from all the Member States and other parties Europol works with. This
duality creates a situation for Europol that if the first part of the cycle is not
successful it directly impacts the second part and decreases value in Europol’s work.

To summarize, Europol is a facilitator of the Member States, it is dependent on the
information received from them, the manner in which Europol handles that
information has a direct impact on how much value Europol can add to the entire
system of classified information. This state of affairs leads back to the question: what
are the implications of Member States’ “chief” position in the decision-making
process throughout the classification cycle?

There are two main perspectives to answer this question. Firstly, the context in which
Europol operates is governed by the openness imperative which in the EU is of
constitutional status stipulated by Article 15 of the Treaty on the Functioning of the
European Union and Article 42 of the Charter of Fundamental Human Rights
granting an individual right of access to documents. These provisions should be read
in conjunction with Article 1 TEU that “decisions are taken as openly as possible”
and Article 10 TEU ensuring that every citizen has a right to participate in the
democratic life of “as openly as possible” Union. Secondly, the objective of Europol is
to maintain operational flexibility which means that informed decisions are taken for
investigations, information is exchanged in a secure yet expeditious fashion and
lastly information can be used in judicial proceedings.

Both perspectives, openness and operational flexibility, can be concretely elaborated
through the mechanism of review. A review of the classification system seeks to
promote both the effective protection of information where warranted and the
disclosure of information where there is not a well-founded basis for protection. Namely, a review of the classification system implies a check of the system. The review of classification system is a crucial instrument to ensure the security of the system but also check that there is no overclassification or compartmentalization of information making it a valuable tool through which accountability of actions is ensured. A review serves the purpose to make proposals for reform in order to reduce the volume of information classified and thereby to strengthen the protection of legitimately classified information, as well as to improve existing personnel security procedures (Report of the Commission on Protecting and Reducing Government Secrecy, 1997).

The review can be internally organized such as for security reasons done by the security unit within Europol or it can be an external check for reasons of compliance and accountability. When it comes to personal data, Europol is reviewed by the Europol Joint Supervisory Body which is an independent body and ensures compliance with the data protection regime.

A review of the classification system in Europol happens only internally through the Security unit (Interview E4). Although legally, the Europol Confidentiality Decision stipulates that review may be conducted by the Council, this has not been the case (Interview E1, E2, E4). The Security unit however does not conduct a review on a “structural basis if there is over or under classification” (Interview E4). They see themselves as “custodian of the information” but not on every individual level. There is an annual revision for the higher classified information, i.e. classified as restricted and above. The Security unit also conducts a review every 5 years, usually to determine if documents should be declassified. This type of review is steered towards improving the protection of classified information and the originators are consulted. It serves, therefore, more towards the direction to enhance operational flexibility.

A democratic review by the European Parliament is not present. This is due to the current competences of the EP in regards to Europol as a result of pre-Lisbon Europol Decision by the Council. Namely, the EP has no authority to check directly Europol for the classification system. The Europol Director is obliged to appear
before the EP but questions regarding the classification system cannot be raised with
great success considering that the EP has no direct access to classified information.
The only mechanism available for the EP which can have drastic consequences is the
adoption of the budget. ‘The threat to refuse or delay the discharge of a budget can
be used as a tool to request chances to a policy, procedures, or activities’
(Parliamentary Oversight of security and intelligence agencies in the European
Union, 2011). As strong as this tool is, nevertheless, it does not tackle the issues of
classification as such and in a sense does not create positive effects since the EP
cannot recommend changes of the classification per se. Additionally, it is highly
unlikely that only due to classification issues the EP would not approve the budget of
Europol.

Yet discussing review seems premature considering that the EP does not even have
access to classified information and Europol treats it as a general public. This is a
result of Regulation No. 1049/01 which stipulates that the legal basis for the EP to
have access to classified documents is to be arranged through an inter-intuitional
agreement (Regulation No.1049/01, 2001). As Europol is not formally an institution
there are no arrangements between the European Parliament and Europol for access
to classified information (Parliamentary Oversight of security and intelligence
agencies in the European Union, 2011). Even if there would have been review, be that
from the Council or the EP, another more fundamental question arises: what can be
the outcome?

If Europol is conditioned by the will of the Member States and it has to follow their
instructions for all actions concerning classification, can Europol actually be held to
account for having made the right decisions or not? And secondly, even if reforms
are suggested, are these in the hands of Europol?

These questions lead to two principle concerns. First, there is no review apart from
the internal one which is more focused on security issues. This is insufficient
especially in light of the fact that national law regulates, inter alia, the access and
sharing of information, the use of coercive powers on the basis of information from
operations coordinated by Europol while as it remains unclear if and to what extent
national bodies, including parliaments, oversee activities of their own state’s
authorities and employees that have a connection with Europol (Parliamentary Oversight of security and intelligence agencies in the European Union, 2011).

Secondly, even if there is internal review, little is in Europol’s power to change the modus of operation. Europol relies to a large extent on information provided by national authorities, parts of its work are carried out by seconded employees of Member States, and ultimately, it is national authorities that implement measures on the basis of Europol’s work —all of these activities are primarily regulated by national law (Parliamentary Oversight of security and intelligence agencies in the European Union, 2011). Hence, if there is overclassification or compartmentalization of information, if there is lack of operational flexibility and the information is classified higher than it should have been leading to negative consequences in the judicial proceedings, Europol has a cloak behind which it self-protects and justifies: the originator makes the decision.

6. Conclusions

Protecting and exchanging sensitive information is crucial for security in the European Union where there are multiple actors engaged in a common goal of ‘a secure Europe in a better world’. Europol, a law enforcement agency, stands as a broker in the midst of the exchange of classified information both within the EU and towards the outside. Yet, Europol has little decision-making power when it comes to choosing information to be classified, the level of classification or its duration. Moreover, Europol to a large extent merely facilitates the process of access and exchange of classified information. Member States, the original classifier in 95% of the overall classified documents, condition Europol’s work by their consent, decision, and action. Irrespective of the normative issues such as trust or efficiency matters that lead to the disproportion between Europol’s activities and its full power over them, this situation has created space for Europol to have a sophisticated secrecy mechanism without holding complete accountability over it. This is particularly evident when two key imperatives for Europol’s undertakings – the principle of openness and operational flexibility – are judged against the mechanism of review of the classification system.
The current state of affairs leads to two main conclusions. Firstly, the Member States, at times reluctantly share their secrets with Europol but at all times maintain the final authority over them. This leads to the second conclusion, namely, Europol has a sophisticated system of secrecy in order to facilitate the security needs of the Member States, hence the EU as well, which takes place without serious review be that for the constitutional requirement of openness or for security necessity of operational flexibility. Hence, the classification system in Europol requires consideration for serious and fundamental reforms in the upcoming changes of Europol’s legal status to be adopted by EU’s legislator.
Bibliography
Council (2009), Council decision 2009/371/JHA of 6 April 2009 establishing the European Police Office


Europol (2009), Decision of the Management Board of Europol of 8 July 2009 laying down the rules concerning access to Europol documents EDOC 360875 v 9 File no. 3550-95r3.


