Foreign Intelligence Gathering Laws

Belgium • France • Germany • Portugal • Romania
Netherlands • Sweden • United Kingdom
European Union

June 2016

Contents

Comparative Summary

Peter Roudik
Director of Legal Research

This report, prepared by foreign law specialists and analysts of the Law Library of Congress, offers a review of laws regulating the collection of intelligence in the European Union (EU) and selected EU Member States, namely Belgium, France, Germany, Netherlands, Portugal, Romania, Sweden, and the United Kingdom, and updates a report on the same topic issued by the Law Library of Congress in 2014. The previous survey of French legislation was substantially amended because of France's new Law on Intelligence, which was passed in 2015. The most recent decisions of the European courts concerning mass surveillance and the validity of data retention activities undertaken by the European countries' governments are reviewed in the EU survey, and measures aimed at the protection of personal data prescribed by a recently concluded US–EU agreement are analyzed. The individual country surveys also describe legislative proposals currently under consideration in the respective parliaments. These include the Investigatory Powers Bill in the United Kingdom, the Cybersecurity Law of Romania, and proposals to enhance the privacy of citizens' communications in the Netherlands.

Because issues of national security are under the jurisdiction of individual EU Member States and are regulated by domestic legislation, individual country surveys provide examples of how the European nations control activities of their intelligence agencies and what restrictions are imposed on information collection. All EU Member States follow EU legislation on personal data protection, which is a part of the common European Union responsibility. The report concludes with a comprehensive overview of applicable EU legislation.

The surveys demonstrate efforts undertaken by individual countries to maintain a balance between law enforcement and national security needs on the one hand and rights to privacy and personal data protection on the other. There is no single, comprehensive legal regime that applies to matters of surveillance, interception of communications, and privacy protection in the countries surveyed. In all of the countries included in the report, intelligence functions are divided among general intelligence and security services, military and financial intelligence, and the police. While in some countries (Belgium, Netherlands, Portugal, and the United Kingdom) intelligence agencies work according to principles established by a comprehensive statute, in others (Germany, Romania, and Sweden) individual laws address specific issues for particular intelligence agencies, and separate legislative or regulatory acts authorize certain government institutions to conduct specific intelligence gathering activities. The report on France demonstrates the country's ongoing transition to regulating the work of intelligence-collection agencies through a major law, as opposed to the prior approach of regulating such work through various executive decisions.

While the legislative bodies of the surveyed countries conduct general oversight of their respective intelligence agencies, parliamentary involvement varies greatly. Judicial oversight is generally limited to the consideration and issuance of warrants for surveillance. Special government bodies for reviewing the legality of interception surveillance and privacy issues have

also been created. These special bodies focus on how information is stored, shared among security agencies within the country and abroad, destroyed, and made available to interested individuals. Limitations on intelligence collection are established by national constitutions, criminal procedure laws, and special legislation, and are aimed at the general defense of rights and freedoms. They include restrictions in terms of the scope, duration, and subject matter of surveillance activities. The use of special powers, including communications surveillance, requires express permission from the Minister of Interior (Netherlands), issuance of a judicial order (Romania), or an approval warrant authorized by the Secretary of State (United Kingdom).

All national laws of the surveyed countries provide for some checks to preserve individuals' personal data and the privacy of electronic and telecommunications, and transpose European Union directives into domestic law. At the same time, these measures are not always effective with regard to privacy protection.

Belgium

Nicolas Boring
Foreign Law Specialist

SUMMARY The Law of 30 November 1998 Organizing the Intelligence and Security Services, as most recently amended in April 2016, establishes the general legislative framework within which Belgium's intelligence agencies operate.

The Law of 30 November 1998 divides intelligence-gathering methods into three categories: "ordinary methods," "specific methods" and "exceptional methods." Ordinary methods tend to have the least impact on citizens' privacy and may generally be used without authorization. If ordinary methods are insufficient, intelligence services may employ specific methods, which involve more extensive encroachments into privacy. Finally, exceptional methods, which are the most intrusive, may only be used to counter a grave threat. Attorneys, medical doctors, and journalists benefit from additional legal protections against the use of specific methods and exceptional methods.

The interception of communications falls into the category of exceptional methods. Such measures must be proportional to the seriousness of the threat and must be authorized by a special oversight commission. Service providers and network operators are required to cooperate with the intelligence agencies for the interception of communications. While the refusal to cooperate is punishable by fine, those who cooperate actively with the operation are offered monetary compensation. It appears that the service providers and network operators may not use or make available any form of encryption that they are not able to decrypt themselves.

Oversight of intelligence gathering is principally provided by an independent administrative commission. In addition to this administrative commission, the Belgian Parliament also oversees intelligence agencies through its Standing Intelligence Agencies Review Committee, which monitors and evaluates the legality of the methods used as well as their effectiveness.

I. Introduction

Belgium has two main intelligence services: the Sûreté de l'Etat (State Security) and the Service general du renseignement et de la sécurité (SGRS, General Intelligence and Security Service).[1] The Sûreté de l'Etat is a civilian intelligence and security service that falls under the authority of the Minister of Justice, although it sometimes also works for the Minister of the Interior.[2] By

[1] *Que sont les services belges de renseignement et de sécurité?* [*What Are the Belgian Intelligence and Security Services?*], COMITÉ PERMANENT DE CONTRÔLE DES SERVICES DE RENSEIGNEMENTS ET DE SÉCURITÉ [BELGIAN STANDING INTELLIGENCE AGENCIES REVIEW COMMITTEE], http://www.comiteri.be/index.php/fr/34-pages-fr/297-que-sont-les-services-belges-de-renseignement-et-de-securite (last visited June 9, 2016), *archived at* https://perma.cc/ZT8F-JHYR, English version *at* http://www.comiteri.be/index.php/en/39-pages-gb/305-what-do-intelligence-and-security-services-stand-for, *archived at* https://perma.cc/TYA7-AGX2.

[2] *Id.*

contrast, the SGRS focuses on military intelligence, and falls under the authority of the Minister of Defense.[3]

In addition, an interagency body was created in 2006 to assess the threat posed by terrorists and extremists against Belgium.[4] This body, called the Organe de coordination pour l'analyse de la menace (OCAM, Coordination Unit for Threat Assessment), is placed under the joint authority of the Minister of the Interior and the Minister of Justice, and relies on information provided to it by the Sûreté de l'Etat, the SGRS, local and federal police, customs and tax authorities, the federal service for foreign affairs, and other Belgian government agencies.[5] The OCAM then provides its analysis back to the agencies responsible for national security, so that they may act on the information as appropriate.[6]

II. Legislative Framework

The legislative framework within which Belgian intelligence agencies operate is principally provided by the Law of 30 November 1998 Organizing the Intelligence and Security Services (Loi du 30 novembre 1998 organique des services de renseignement et de sécurité).[7] This Law has been amended several times since its initial adoption in 1998, with the most recent amendment occurring in April 2016.[8] It applies to both agencies, and requires them to "respect and contribute to the protection of individual rights and freedoms, as well as to society's democratic development."[9] Toward that purpose, this Law provides a basic legal framework for intelligence-gathering activities.

The Law of 30 November 1998 divides intelligence-gathering methods into three categories: ordinary, specific, and exceptional.[10] "Ordinary methods" appear to be those that have the least impact on the privacy of Belgian citizens and residents, such as consulting publicly-available information, accessing and observing public spaces, obtaining information from human sources, or asking an electronic communications service provider about the identity of one of its

[3] *Id.*

[4] *Qu'est-ce que l'Organe de coordination pour l'analyse de la menace?* [*What Is the Coordination Unit for Threat Assessment?*], COMITÉ PERMANENT DE CONTRÔLE DES SERVICES DE RENSEIGNEMENTS ET DE SÉCURITÉ [BELGIAN STANDING INTELLIGENCE AGENCIES REVIEW COMMITTEE] (last visited June 9, 2016), http://www.comiteri.be/index.php/fr/34-pages-fr/298-qu-est-ce-que-l-organe-de-coordination-pour-l-analyse-de-la-menace, *archived at* https://perma.cc/5PQ7-4B8N.

[5] *Id.*

[6] *Id.*

[7] Loi organique du 30 novembre 1998 des services de renseignement et de sécurité [Organizational Law of 30 November, 1998, Organizing the Intelligence and Security Services], http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=1998113032, *archived at* https://perma.cc/4C9Z-L9V7.

[8] Loi du 21 avril 2016 portant des dispositions diverses Intérieur. – Police intégrée [Law of 21 April 2016 Establishing Miscellaneous Interior Provisions. – Integrated Police] arts. 17–23, http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=2016042106, *archived at* https://perma.cc/U4UK-A58L. .

[9] Loi du 30 novembre 1998, art. 2.

[10] *Id.* arts. 14–18/17.

subscribers.[11] These methods may generally be used by the agents of the intelligence agencies as a routine matter, without specific authorization. "Specific methods" involve more extensive encroachment into privacy, such as observing public spaces with the help of technical devices (which probably refers to microphones and recording devices), surveilling private spaces, identifying the sender and/or recipient of a postal letter or package, or asking an electronic communications service provider about the payment methods and timing of one of its subscribers.[12] These intelligence-gathering methods may only be used if they are proportional to the potential threat being investigated and if ordinary methods are insufficient to obtain the information needed.[13] Furthermore, specific methods may only be employed with the written authorization of the intelligence agency's leader and after notifying a special oversight commission.[14] Finally, "exceptional methods" are those that are the most intrusive on privacy, such as accessing computer systems; collecting information on bank accounts and bank transactions; or intercepting, listening to, and/or recording private communications.[15] Deceitful practices such as having agents use fake identities are also considered exceptional methods.[16] Exceptional methods must be used in a way that is proportional to the seriousness of the threat, and may only be used to counter a grave threat.[17] Furthermore, an exceptional method may only be used if ordinary and specific methods are insufficient, and after obtaining prior approval from the special oversight commission.[18]

Special protections exist for attorneys, doctors, and journalists. If a specific or exceptional method is deployed against a member of these professions, the president of the target's professional organization (the Bar for attorneys, the National Council of the Medical College for doctors, or the Professional Journalists' Association for journalists) must be informed.[19] Furthermore, an exceptional method may only be deployed against a member of these professions if there is serious evidence that he/she has actively and personally participated in the grave threat being investigated.[20]

[11] *Id*. art. 14–18.

[12] *Id*. art. 18/2.

[13] *Id*. art. 18/3.

[14] *Id*.

[15] *Id*. art. 18/2.

[16] *Id*.

[17] *Id*. art. 18/9.

[18] *Id*.

[19] *Id*. art. 18/2.

[20] *Id*. art. 19/9.

III. Interception of Communications

Article 18/17 of the Law of 30 November 1998 provides that intelligence services may "listen to, gain knowledge of, and record communications" in order to fulfill their missions.[21] Since secretly accessing, listening to, or recording private communications fall into the exceptional method category described above, an intelligence service must obtain prior authorization from the special oversight commission before employing these measures.[22] When an intelligence service has obtained the required authorization to conduct this kind of surveillance on an electronic communications network, it can serve a written demand to the network operator or the service provider, upon which the network operator or service provider is required to give technical assistance to the intelligence service.[23] Any person who refuses to give technical assistance pursuant to a properly-authorized demand is punishable by a fine of between €26 and €10,000 (about US$30 to US$11,364).[24] On the other hand, companies and individuals who cooperate in giving technical assistance are paid for their services on the basis of government-established rates.[25]

The principal statute governing electronic communications in Belgium requires that network operators as well as end users be capable of allowing the authorities to "listen to, gain knowledge of, and record" communications.[26] A Royal Order from 2010 includes electronic communications service providers alongside network operators as being required to have the technical ability to provide clear and readable (decoded, decompressed, and decrypted) copies of communications requested by Belgian intelligence services.[27] It appears, in other words, that service providers and network operators may not use or make available any form of encryption that they would be unable to decrypt themselves.

IV. Oversight

The Law of 30 November 1998 created an administrative commission to oversee the activities of the Sûreté de l'Etat and the SGRS.[28] As discussed in Part II above, this administrative commission must be notified every time an intelligence service employs a specific method, and its prior approval is necessary for an intelligence service to use an exceptional method. The

[21] *Id.* art. 18/17.

[22] *Id.* art. 43/1.

[23] *Id.* art. 18/17.

[24] *Id.*

[25] *Id.* art. 18/18.

[26] Loi du 13 juin 2005 relative aux communications électroniques [Law of June 13, 2005, Regarding Electronic Communications] art. 127, http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2005061332&table_name=loi, *archived at* https://perma.cc/92QM-7E5S.

[27] Arrêté royal du 12 octobre 2010 déterminant les modalités de l'obligation de collaboration légale en cas de demandes concernant les communications électroniques par les services de renseignement et de sécurité [Royal Order of October 12, 2010, Establishing the Conditions of the Obligation of Lawful Collaboration in Cases of Demands by Intelligence and Security Services Regarding Electronic Communications] art. 8, http://www.ejustice.just.fgov.be/cgi_loi/loi_a.pl, *archived at* https://perma.cc/5ZG7-VUL9.

[28] *Id.* art. 43/1.

commission is independent, and is composed of three members and three alternates.[29] Two of the three members, and two of the alternates, must be judges.[30] The commission members are appointed for a period of five years, renewable twice.[31]

In addition to the administrative commission, oversight over both intelligence agencies is exercised by the Belgian Parliament through the Comité permanent de contrôle des services de renseignements et de sécurité (Standing Intelligence Agencies Review Committee), also known as the Comité permanent R (R Standing Committee).[32] This Committee monitors and assesses the legality of the means employed by the Belgian intelligence agencies.[33] Additionally, this Committee evaluates the effectiveness of Belgian intelligence as well as the level of coordination between the intelligence agencies.[34] The R Standing Committee publishes yearly reports on its activity (though the latest available one, as of the writing of this report, is for 2014).[35] It also publishes some of its investigative reports[36] and a few of its advisory opinions.[37]

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] *Mission* [*Role*], COMITÉ PERMANENT DE CONTRÔLE DES SERVICES DE RENSEIGNEMENTS ET DE SÉCURITÉ [BELGIAN STANDING INTELLIGENCE AGENCIES REVIEW COMMITTEE], http://www.comiteri.be/index.php/fr/comite-permanent-r/mission (last visited June 9, 2016), *archived at* https://perma.cc/4ZDZ-V3RF, English version *at* http://www.comiteri.be/index.php/en/standing-committee-i/role, *archived at* https://perma.cc/7RSH-5SW9.

[33] *Id.*

[34] *Id.*

[35] *Rapports d'activité* [*Activity Reports*], COMITÉ PERMANENT DE CONTRÔLE DES SERVICES DE RENSEIGNEMENTS ET DE SÉCURITÉ [BELGIAN STANDING INTELLIGENCE AGENCIES REVIEW COMMITTEE], http://www.comiteri.be/index.php/fr/publications/rapports-dactivites-3 (last visited June 10, 2016), *archived at* https://perma.cc/TSD6-MSYE, English version *at* http://www.comiteri.be/index.php/en/publications/activity-reports, *archived at* https://perma.cc/SKF8-C9B2.

[36] *Rapports d'enquêtes* [*Investigation Reports*], COMITÉ PERMANENT DE CONTRÔLE DES SERVICES DE RENSEIGNEMENTS ET DE SÉCURITÉ [BELGIAN STANDING INTELLIGENCE AGENCIES REVIEW COMMITTEE], http://www.comiteri.be/index.php/fr/publications/rapports-denquetes-3 (last visited June 10, 2016), *archived at* https://perma.cc/HYY3-A64U, English version *at* http://www.comiteri.be/index.php/en/publications/investigation-reports, *archived at* https://perma.cc/88K2-58XA.

[37] *Avis* [*Advice*], COMITÉ PERMANENT DE CONTRÔLE DES SERVICES DE RENSEIGNEMENTS ET DE SÉCURITÉ [BELGIAN STANDING INTELLIGENCE AGENCIES REVIEW COMMITTEE], http://www.comiteri.be/index.php/fr/publications/avis (last visited June 10, 2016), *archived at* https://perma.cc/LE62-6VDS, English version *at* http://www.comiteri.be/index.php/en/publications/advice, *archived at* https://perma.cc/2NF6-8XRY.

France

Nicolas Boring
Foreign Law Specialist

SUMMARY While a number of intelligence agencies operate in France, large-scale communications interception is carried out primarily by the Directorate General on Exterior Security under the Ministry of Defense, and the metadata collected is shared within the French intelligence network. All of the existing intelligence agencies were originally created by executive action. The adoption of the Law on Intelligence, promulgated in July 2015, establishes a coherent and comprehensive legislative framework to regulate the activities of the intelligence agencies.

The interception of communications is principally governed by the Code of Domestic Security, as amended by recent laws such as the Law on Intelligence and the Law on International Electronic Communications Measures. The legislation recognizes privacy guarantees but also provides for the interception of communications in circumstances where national security and other safety-related concerns are at issue. The Prime Minister may authorize interception when proposed by specified ministers. Such authorizations are time limited. The information collected must be destroyed when no longer needed for a recognized purpose. Intelligence agencies may also obtain certain technical information directly from telephone and Internet service providers. Oversight of interception surveillance is provided by the National Commission for the Control of Intelligence Techniques, but this Commission's recommendations do not appear to be binding. Parliamentary requests for classified information are routinely rejected and the French Parliament has no inherent right to hear or question members of the intelligence services.

I. Introduction

The legislative framework for French intelligence services has changed drastically in the last year. Up until July 2015, France was one of the only Western democracies without a comprehensive and coherent legal framework to govern the activities of its intelligence services.[1] Addressing this issue, the French government adopted the Law on Intelligence on July 24, 2015.[2] The provisions of this Law were incorporated into the existing codes of French law, mainly the Code de la sécurité intérieur (Code of Domestic Security).

France has six intelligence agencies. Three fall under the authority of the Ministry of Defense: the Direction générale de la sécurité extérieure (DGSE, Directorate General on Exterior Security),

[1] Press Release, Premier Ministre [Office of the Prime Minister], Projet de loi renseignement, "Protéger les Français dans le respect des libertés" [Intelligence Bill, "Protecting the French People and Respecting Freedoms"] at 7 (Mar. 19, 2015), http://www.gouvernement.fr/partage/3691-projet-de-loi-renseignement-proteger-les-francais-dans-le-respect-des-libertes, *archived at* https://perma.cc/B4PC-7TY6.

[2] Loi No. 2015-912 du 24 juillet 2015 relative au renseignement (1) [Law No. 2015-912 of 24 July 2015 Regarding Intelligence (1)], https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899&categorieLien=id, *archived at* https://perma.cc/6G4H-AKLP.

the Direction du renseignement militaire (DRM, Directorate on Military Intelligence), and the Direction de la protection et de la sécurité de la défense (DPSD, Directorate on Defense Protection and Security). Two agencies fall under the authority of the Ministry of Finance: the Cellule de traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN, Service Against the Laundering of Capital and the Financing of Terrorism) and the Direction nationale du renseignement et des enquêtes douanières (DNRED, National Directorate on Customs Intelligence and Investigations). Finally, the Ministry of the Interior has an intelligence service as well, the Direction centrale du renseignement intérieur (DCRI, Central Directorate on Domestic Intelligence).[3]

It appears that large-scale communications interception is done mainly by the DGSE, which systematically collects all telephone and electronic communications metadata in France, according to news reports.[4] The DGSE appears to share the collected metadata with the other French intelligence agencies.[5]

II. Legislative Framework

The six main intelligence agencies mentioned above were all created by decisions of the executive branch rather than by legislation. The DGSE, DPSD, DRM, DCRI, and TRACFIN were all created by decrees, and the DNRED was created by an *arrêté* (executive decision).[6] Only in 2011 did the French Parliament provide some legislative basis for the creation of these agencies, by adopting a law stating that "specialized intelligence services . . . are appointed by executive decision of the Prime Minister."[7]

Prior to the adoption of the Law on Intelligence, French intelligence agencies operated within an ill-defined legal framework. A 2013 parliamentary report had noted that many of France's intelligence agencies operated in a very blurry "paralegal" or "extralegal" environment, despite

[3] COMMISSION DES LOIS CONSTITUTIONNELLES, DE LA LEGISLATION ET DE L'ADMINISTRATION GENERALE DE LA REPUBLIQUE [COMMISSION ON CONSTITUTIONAL LAWS, LEGISLATION, AND GENERAL ADMINISTRATION OF THE REPUBLIC], ASSEMBLEE NATIONALE [NATIONAL ASSEMBLY], RAPPORT D'INFORMATION [INFORMATION REPORT], No. 1022, at 10–11 (May 14, 2013).

[4] Jacques Follorou & Franck Johannes, *Révélations sur le Big Brother français* [*Revelations on the French Big Brother*], LE MONDE (July 4, 2013), http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html, *archived at* https://perma.cc/YJ7J-XGLU.

[5] *Id.*

[6] COMMISSION DES LOIS CONSTITUTIONNELLES, DE LA LEGISLATION ET DE L'ADMINISTRATION GENERALE DE LA REPUBLIQUE, *supra* note 3, at 15–16.

[7] Loi No. 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure [Law No. 2011-267 of March 14, 2011, of Orientation and Programming for the Performance of Domestic Security] art. 27, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707312& categorieLien=id, *archived at* https://perma.cc/Q3TX-PAX9 . This provision was incorporated into the French Code de la défense (Defense Code) as article L2371-1, http://www.legifrance.gouv.fr/affichCode.do;jsessionid=6D0EC48E6013B6B33D2E5AD1A7AC622E.tpdjo10v_3?idSectionTA=LEGISCTA000023710864&cidTexte=LEGITEXT000006071307&dateTexte=20141204, *archived at* https://perma.cc/CN49-HXEQ.

some efforts by the legislative branch to provide a better framework.[8] The regulation of French intelligence agencies rested on many decrees, executive decisions, circulars, and instructions that are classified.[9] These regulations (decrees, executive decisions, etc.) do not have the same legal authority as duly enacted legislation.

The Law on Intelligence aims to establish a unified legal framework for the activities of intelligence services.[10] Although the adoption of the Law was probably accelerated by the intensity of the threat of terrorism and, in particular, the January 2015 attacks in France, the government emphasized that it was the result of thorough reflection and not enacted under the pressure of any specific urgent situation.[11]

The Law on Intelligence has two main objectives. First, the Law aims to strengthen the means of action of intelligence agencies by authorizing intelligence services to use newly developed techniques as well as techniques that were previously reserved for the police, such as location tracking, interception of communications, and covert sound recording ("bugging").[12] Second, the Law aims to guarantee the protection of civil liberties and the right to privacy. By establishing a precise legal framework that authorizes intelligence agencies to use the necessary techniques for intelligence gathering, the Law ensures a balance between the reinforced security of citizens and the protection of their individual freedoms.[13]

The Law on Intelligence authorizes intelligence agencies to exercise their powers exclusively in those cases that the law deems as necessary for reasons of public interest, within the limits prescribed by law, and with respect for the principle of proportionality.[14] Furthermore, the Law defines the missions that the intelligence agencies may pursue and states the exclusive purposes

---

[8] COMMISSION DES LOIS CONSTITUTIONNELLES, DE LA LEGISLATION ET DE L'ADMINISTRATION GENERALE DE LA REPUBLIQUE, *supra* note 3, at 13.

[9] *Id.* at 17.

[10] JEAN-JACQUES URVOAS, RAPPORT FAIT AU NOM DE LA COMMISSION DES LOIS CONSTITUTIONNELLES, DE LA LEGISLATION ET DE L'ADMINISTRATION GENERALE DE LA REPUBLIQUE APRES ENGAGEMENT DE LA PROCEDURE ACCELEREE, SUR LE PROJET DE LOI (NO. 2669) RELATIF AU RENSEIGNEMENT [REPORT PREPARED ON BEHALF OF THE COMMISSION ON CONSTITUTIONAL LAWS, ON LEGISLATION AND ON THE GENERAL ADMINISTRATION OF THE REPUBLIC, AFTER ACTIVATION OF THE ACCELERATED PROCEDURE, ON BILL (NO. 2669) REGARDING INTELLIGENCE], ASSEMBLEE NATIONALE 14 (Apr. 2, 2015), http://www.assemblee-nationale.fr/14/rapports/r2697.asp#P31784757, *archived at* https://perma.cc/B4VF-YN3L.

[11] Press Release, *supra* note 1, at 8.

[12] *Recommandation sur le projet de loi relatif au renseignement* [*Recommendation on the Bill Regarding Intelligence*], ASSEMBLEE NATIONALE, http://www2.assemblee-nationale.fr/14/autres-commissions/numerique/a-la-une/recommandation-sur-le-projet-de-loi-relatif-au-renseignement (last visited June 10, 2016), *archived at* http://perma.cc/AWB4-KUGP.

[13] *Id.*; *La lutte contre le terrorisme* [*The Fight Against Terrorism*], GOUVERNEMENT.FR (May 23, 2016), http://www.gouvernement.fr/action/la-lutte-contre-le-terrorisme, *archived at* https://perma.cc/K63Z-S2SX.

[14] Loi No. 2015-912 du 24 juillet 2015 relative au renseignement art. 1; CODE DE LA SECURITE INTERIEURE art. L801-1, https://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=D47CAB6F4EC7ADA9A26549DF79664673.tpdila23v_2?idArticle=LEGIARTI000030934657&cidTexte=LEGITEXT000025503132&dateTexte=20160610, *archived at* https://perma.cc/3DGZ-PL8M.

for which the intelligence services may justify the use of their powers.[15] The Law also specifies the conditions under which each intelligence-gathering technique may be used.[16]

III. Interception of Communications

Before the adoption of the Law on Intelligence, the interception of communications was already governed by certain provisions of the Code of Domestic Security. However, the Law on Intelligence substantially broadens the legal framework surrounding the interception of communications and the collection of metadata.[17] Furthermore, another law was adopted in November 2015 to govern the interception of electronic correspondence emitted or received abroad.[18] Like the provisions of the Law on Intelligence, the provisions of this law on interception were also incorporated into the Code of Domestic Security.

The right to privacy, particularly the secrecy of correspondence, is in principle guaranteed by the Code.[19] Privacy may only be violated by the government when it is necessary and in the public interest, as defined by law.[20] Consequently, intelligence agencies may only exercise their powers to

- protect national independence, the integrity of the territory, and provide for the national defense;
- defend major interests in foreign policy and the execution of France's commitments to Europe and internationally;
- prevent all forms of foreign interference;
- defend the major economic, industrial, and scientific interests of France;
- prevent terrorism;
- prevent attacks on the republican form of institutions;

[15] URVOAS, *supra* note 10, at 14; Loi No. 2015-912 du 24 juillet 2015 relative au renseignement art. 2; CODE DE LA SECURITE INTERIEURE arts. L811-1 to L811-3, https://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000030935034&cidTexte=LEGITEXT000025503132&dateTexte=20160610, *archived at* https://perma.cc/4LRT-2NFK.

[16] URVOAS, *supra* note 10, at 14; Loi No. 2015-912 du 24 juillet 2015 relative au renseignement arts. 1–3; CODE DE LA SECURITE INTERIEURE arts. L811-3, & L821-1 to L821-8, https://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000030935046&cidTexte=LEGITEXT000025503132&dateTexte=20160610, *archived at* https://perma.cc/F9F9-MT6M.

[17] ASSEMBLEE NATIONALE, *supra* note 12.

[18] Loi No. 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales (1) [Law No. 2015-1556 of 30 November 2015 Regarding International Electronic Surveillance Measures (1)], https://www.legifrance.gouv.fr/eli/loi/2015/11/30/DEFX1521757L/jo/texte, *archived at* https://perma.cc/968G-CG4V.

[19] CODE DE LA SECURITE INTERIEURE art. L801-1.

[20] *Id.*

- prevent actions for the maintenance or reorganization of banned groups, such as armed militias, terrorist organizations, or hate groups;
- prevent collective violence that greatly disrupts public peace;
- prevent crime and organized crime; and
- prevent the proliferation of weapons of mass destruction.[21]

It appears that the term "electronic communications" includes communications by telephone, fax, and email.[22] The authorization to intercept electronic communications may be given only by written order of the Prime Minister; by direct collaborators entitled to national defense secrets who are specifically chosen by the Prime Minister, upon the written and reasoned proposal of either the Minister of Defense, Minister of the Interior, or Minister in Charge of Customs; or by direct collaborators specifically chosen by these ministers.[23] This authorization is valid for a maximum of four months, but may be renewed by the same procedure under which it was initially granted.[24] Only information relevant to one of the purposes provided by the Code and enumerated above may be transcribed from the intercepted communications, and any recording must be destroyed after thirty days.[25] Transcriptions must be destroyed as soon as they are no longer necessary for the purposes enumerated above.[26] Furthermore, the Prime Minister sets, by decree, the maximum number of communications interceptions that may be simultaneously conducted at any given time.[27] This number was set at 2,700 in 2015.[28]

The Law also extends the possible target of an interception to include people close to the individuals for whom an authorization was given, if there are serious reasons to believe that they can supply information.[29] Intelligence agencies may also obtain directly from telephone and Internet service providers the type of technical information that may be found on a telecommunications bill: the service subscriber's identity, the location of the subscriber's

[21] *Id.* art. L811-3.

[22] COMMISSION DES LOIS CONSTITUTIONNELLES, DE LA LEGISLATION ET DE L'ADMINISTRATION GENERALE DE LA REPUBLIQUE, *supra* note 3, at 18–22.

[23] CODE DE LA SECURITE INTERIEURE art. L821-2, https://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000030935046&cidTexte=LEGITEXT000025503132&dateTexte=20160610, *archived at* https://perma.cc/DTH8-39UG.

[24] *Id.* art. L821-4.

[25] *Id.* arts. L822-2 & L822-3, https://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000030935064&cidTexte=LEGITEXT000025503132&dateTexte=20160610, *archived at* https://perma.cc/E5XC-XHHU.

[26] *Id.* art. L822-3.

[27] *Id.* art. L852-1, https://www.legifrance.gouv.fr/affichCode.do;jsessionid=1C72447446E6D4F800C3DBF629B8697A.tpdila23v_2?idSectionTA=LEGISCTA000030935846&cidTexte=LEGITEXT000025503132&dateTexte=20160611, *archived at* https://perma.cc/A839-EYBD.

[28] *Comptes rendus de la CE autorités administratives indépendantes* [*Minutes of the Fact-Finding Commission on Independent Administrative Authorities*], SÉNAT [SENATE] (Sept. 16, 2015), http://www.senat.fr/compte-rendu-commissions/20150914/ce_aai.html, *archived at* https://perma.cc/8KQV-V42D.

[29] CODE DE LA SECURITE INTERIEURE art. L852-1.

terminal equipment, the calls made and/or received, and the date and duration of these communications.[30]

Interception of communications emitted or received outside of France may be authorized for the purpose enumerated in article L811-3 of the Code of Domestic Security.[31] However, intelligence agencies may not use such a measure as a means to monitor individuals, unless such individuals are communicating from outside of France and pose a threat to the fundamental interests of the nation, or unless an authorization for the interception of their communications within France was already in place.[32] The Prime Minister is to designate, in a reasoned decision, the networks of electronic communications for which the interception of electronic correspondence and data emitted or received outside of France may be authorized.[33]

Other means of covertly gathering intelligence, such as placing microphones ("bugs") in a private location or vehicle, secretly taking pictures or video footage, or capturing computer data, may also be authorized under similar conditions, and following similar procedures, as for the interception of communications.[34] The restrictions imposed by the Code of Domestic Security tend to be somewhat more restrictive for these methods, however. For example, the authorization to place a recording device in a private location is valid for two months instead of four,[35] and the authorization to covertly access data on a computer system is valid only for a period of thirty days.[36]

IV. Oversight

The main body responsible for the oversight of interception surveillance is the Commission nationale de contrôle des techniques de renseignement (CNCTR), National Commission for the Control of Intelligence Techniques).[37] The CNCTR was instituted by the Law on Intelligence, replacing what used to be the Commission nationale pour les interceptions de securité (CNCIS, National Commission for Security Interceptions).[38] Requests for authorizations to intercept a

[30] *Id.* art. L851-1, https://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=1C72447446E6D4F800C3DBF629B8697A.tpdila23v_2?idArticle=LEGIARTI000030935595&cidTexte=LEGITEXT000025503132&dateTexte=20160611, *archived at* https://perma.cc/8NEJ-VFE9.

[31] *Id.* art. L854-1, https://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=1C72447446E6D4F800C3DBF629B8697A.tpdila23v_2?idArticle=LEGIARTI000031552057&cidTexte=LEGITEXT000025503132&dateTexte=20160611, *archived at* https://perma.cc/4J6Z-BTEX.

[32] *Id.*

[33] *Id.* art. L854-2, https://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=1C72447446E6D4F800C3DBF629B8697A.tpdila23v_2?idArticle=LEGIARTI000031550317&cidTexte=LEGITEXT000025503132&dateTexte=20160611, *archived at* https://perma.cc/58TT-D8VL.

[34] *Id.* arts. L853-1 to L853-3, https://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000030935962&cidTexte=LEGITEXT000025503132&dateTexte=20160611, *archived at* https://perma.cc/DS34-NXPR.

[35] *Id.* art. L853-1.

[36] *Id.* art. L853-2.

[37] *Id.* arts. L833-1 to L833-11, https://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000030935094&cidTexte=LEGITEXT000025503132&dateTexte=20160611, *archived at* https://perma.cc/99X3-6P69.

[38] Loi No. 2015-912 du 24 juillet 2015 relative au renseignement art. 21.

person's communications must be sent to the CNCTR, which is to provide its opinion to the Prime Minister.[39] In the case of absolute urgency, and only for reasons concerning national independence, the integrity of the territory and national defense, and the prevention of terrorism or attacks on the republican form of institutions, review by the CNCTR can be omitted, although the CNCTR must still be informed as quickly as possible.[40] The CNCTR's decisions are not legally binding, but if the Prime Minister authorizes an interception of communications contrary to a CNCTR decision, he/she must provide an explanation as to why the CNCTR's advice was not followed.[41] Furthermore, if an intelligence-gathering operation involves breaking into a private residence (for example, to place or retrieve a secret recording device), authorization may not be given without first consulting with the CNCTR.[42] If the Prime Minister decides to authorize the operation after a negative opinion on the part of the CNCTR, the latter may immediately appeal to the Conseil d'Etat (Council of State, the highest administrative court).[43]

The CNCTR is composed of nine members, including two senators and two members of the National Assembly.[44] Beyond these four seats on the CNCTR, parliamentary oversight over intelligence activities appears to be quite weak. Indeed, requests for classified documents from parliamentary committees tend to be rejected, and members of the French Parliament have no general right to hear or question members of the intelligence services.[45]

[39] CODE DE LA SECURITE INTERIEURE art. L821-3.

[40] *Id.* art. L821-5.

[41] *Id.* art. L821-4.

[42] *Id.* art. L853-3.

[43] *Id.*

[44] *Id.* art. L831-1, https://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=1C72447446E6D4F800C3DBF629B8697A.tpdila23v_2?idArticle=LEGIARTI000030935078&cidTexte=LEGITEXT000025503132&dateTexte=20160611, *archived at* https://perma.cc/LVV5-4H2H.

[45] DIRECTORATE-GENERAL FOR INTERNAL POLICIES, EUROPEAN PARLIAMENT, NATIONAL PROGRAMMES FOR MASS SURVEILLANCE OF PERSONAL DATA IN EU MEMBER STATES AND THEIR COMPATIBILITY WITH EU LAW 66 (Oct. 2013), http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf, *archived at* https://perma.cc/XH3M-UGF5.

Germany

Jenny Gesley
Foreign Law Specialist

SUMMARY Germany maintains a strict separation between intelligence and law enforcement/police agencies. Intelligence agencies are therefore prohibited from using police powers to gather information. There are three intelligence agencies at the federal level, two of which focus on domestic intelligence, whereas the third one, the Federal Intelligence Service, focuses on foreign intelligence. Intelligence gathering in Germany is regulated by the acts establishing the three federal intelligence agencies and the Act to Restrict the Privacy of Correspondence, Mail, and Telecommunications. The expanded powers of the law enforcement and police agencies to maintain national security are contained in the Act on the Federal Criminal Police Office, the Act on the Federal Police, the Act on the Customs Investigation Bureau and the Customs Investigation Offices, and the Code of Criminal Procedure. The intelligence and law enforcement agencies may access, intercept, and request stored communications data, subject to limits specified in applicable laws. The intelligence agencies are subject to extensive administrative as well as parliamentary oversight, which includes several specialized parliamentary control panels but also general parliamentary oversight.

I. Introduction

In Germany, the task of maintaining national security is divided between the intelligence and the law enforcement and police agencies. Because Germany is a federation, there are federal as well as state agencies. In addition, there is a strict separation between intelligence and police agencies, although their areas of responsibility might overlap nonetheless.

The strict separation was established after the Second World War in order to prevent an accumulation of police and intelligence powers in an agency like the Nazi's Secret State Police (Gestapo). The Allied Occupation Forces made the separation a precondition of approval of the German Basic Law,[1] the country's constitution, which provides for the establishment of police and law enforcement agencies as well as an intelligence agency.[2] The law therefore states that

[1] Military Governors' Letter to Parliamentary Council Defining Federal Police Power, Apr. 14, 1949, FRUS 1949/III, Doc. No. 98, https://history.state.gov/historicaldocuments/frus1949v03/d98, *archived at* http://perma.cc/4KR9-2QM5; Letter from the Military Governors to Dr. Konrad Adenauer, President of the Parliamentary Council, approving the Basic Law, May 12, 1949, MILITARY GOVERNMENT GAZETTE – GERMANY (BRITISH ZONE), No. 35, Part 2 B at 29, http://germanhistorydocs.ghi-dc.org/pdf/eng/Founding%205%20ENG.pdf, *archived at* http://perma.cc/2E3X-5QA4.

[2] GRUNDGESETZ FÜR DIE BUNDESREPUBLIK DEUTSCHLAND [GRUNDGESETZ] [GG] [BASIC LAW], May 23, 1949, BUNDESGESETZBLATT [BGBL.] [FEDERAL LAW GAZETTE] I at 1, art. 87, http://www.gesetze-im-internet.de/bundesrecht/_gg/gesamt.pdf, *archived at* http://perma.cc/3VDB-NJW4, unofficial English translation *at* http://www.gesetze-im-internet.de/englisch_gg/basic_law_for_the_federal_republic_of_germany.pdf, *archived at* http://perma.cc/MER4-79JH.

the intelligence agencies are not authorized to use force or other types of police powers to gather information.[3]

The three existing federal intelligence agencies are the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz, BfV), the Military Counter-Intelligence Service (Militärischer Abschirmdienst, MAD), and the Federal Intelligence Service (Bundesnachrichtendienst, BND). The BfV and the MAD gather domestic intelligence, whereas the BND focuses on foreign intelligence.

In addition, following the September 11 terrorist attacks and the subsequent terrorist attacks in Madrid and London, federal law enforcement/police agencies were also given preventive powers to protect against "homegrown terrorists," including, among other things, the authority to intercept communications. Agencies granted such powers include the Federal Criminal Police Office,[4] the Federal Police,[5] and the Customs Investigation Bureau and Customs Investigation Offices.[6]

On April 20, 2016, however, the German Federal Constitutional Court ruled that the Act on the Federal Criminal Police Office was partially unconstitutional, because various provisions that deal with the investigative powers of the Federal Criminal Police Office for fighting international terrorism were not proportional. The Court criticized the legal requirements for carrying out covert surveillance measures as too broad and unspecific and held that the norms allowing the transfer of data to third-party authorities and to authorities in third countries lacked sufficient

[3] Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz - BVerfSchG) [Act on the Federal Office for the Protection of the Constitution], Dec. 20, 1990, BGBL. I at 2954, 2970, as amended, § 2, para. 1, sentence 3, § 8, para. 3, http://www.gesetze-im-internet.de/bundesrecht/bverfschg/gesamt.pdf, *archived at* http://perma.cc/C858-Y6VY; Gesetz über den militärischen Abschirmdienst (MAD-Gesetz - MADG) [Act on the Military Counter-Intelligence Service], Dec. 20, 1990, BGBL. I at 2954, 2977, as amended, § 1, para. 4, § 4, para. 2, http://www.gesetze-im-internet.de/bundesrecht/madg/gesamt.pdf, *archived at* http://perma.cc/99CA-LB6W; Gesetz über den Bundesnachrichtendienst (BND-Gesetz - BNDG) [Act on the Federal Intelligence Service], Dec. 20, 1990, BGBL. I at 2954, 2979, as amended, §1, para. 1, sentence 2, § 2, para. 3, sentence 1, http://www.gesetze-im-internet.de/bundesrecht/bndg/gesamt.pdf, *archived at* http://perma.cc/7DTM-H656. Unofficial English translations of all three acts are available at http://www.ennir.be/sites/default/files/pictures/GermanLawsgoverningParliamentaryControlofIntelligenceActivities.pdf, *archived at* http://perma.cc/9VKD-LDJH.

[4] Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Artikel 1 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten) (Bundeskriminalamtgesetz - BKAG) [Act on the Federal Criminal Police Office], July 7, 1997, BGBL. I at 1650, as amended, § 7, paras. 3, 4; § 20b, paras. 3, 4; § 20l; § 20m; § 20m; § 22, http://www.gesetze-im-internet.de/bundesrecht/bkag_1997/gesamt.pdf, *archived at* http://perma.cc/XJ9R-4HUX.

[5] Gesetz über die Bundespolizei (Bundespolizeigesetz - BPolG) [Act on the Federal Police], Oct. 19, 1994, BGBL. I at 2978, 2979, as amended, http://www.gesetze-im-internet.de/bundesrecht/bpolbg/gesamt.pdf, *archived at* http://perma.cc/LEU5-HE59.

[6] Gesetz über das Zollkriminalamt und die Zollfahndungsämter (Zollfahndungsdienstgesetz - ZFdG) [Act on the Customs Investigation Bureau and the Customs Investigation Offices] Aug. 16, 2002, BGBL. I at 3202, as amended, § 7, paras. 5-9; § 15, paras. 2–6; §§ 23a–23g, http://www.gesetze-im-internet.de/bundesrecht/zfdg/gesamt.pdf, *archived at* http://perma.cc/T7J8-T9TV.

legal restrictions. The provisions that were declared unconstitutional will mainly remain in force, subject to restrictions, up to and including June 30, 2018.[7]

In June 2016, in reaction to terrorist attacks in Paris and Istanbul, the Federal Government published a draft act which would amend several laws in order to improve information sharing between national and foreign agencies fighting international terrorism. Among other things, the act would establish a common database for the BfV and foreign intelligence agencies and expand the powers of the BND and of the Federal Police.[8]

II. Intelligences Agencies

A. Federal Office for the Protection of the Constitution (BfV)

The BfV is an executive agency that falls under the authority of the Federal Ministry of the Interior.[9] Its purpose is to protect the free democratic order and the existence and the security of the Federation and the German states.[10] The law provides that the BfV is required to cooperate with its counterparts at the state level to ensure the protection of the constitution.[11]

The agency focuses its work on fighting and collecting information on politically motivated crimes (left- and right-wing extremism); Islamist terrorism and other extremist efforts of foreigners posing a threat to national security; espionage, including cyber espionage and industrial espionage; and the Scientology Organization.[12]

According to section 3 of the Act on the Federal Office for the Protection of the Constitution, the agencies for the protection of the constitution are tasked with the collection and analysis of information, intelligence, and documents relating to individuals or subject matter, concerning

[7] For more information, see Jenny Gesley, *Germany: Federal Constitutional Court Declares Terrorism Legislation Partially Unconstitutional*, GLOBAL LEGAL MONITOR (May 3, 2016), http://www.loc.gov/law/foreign-news/article/germany-federal-constitutional-court-declares-terrorism-legislation-partially-unconstitutional/, *archived at* http://perma.cc/HEM5-JBC8.

[8] Bundesregierung [Federal Government], *Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus* [*Draft Act of the Federal Government, Draft Act to Introduce Improved Information Sharing for the Fight Against International Terrorism*], https://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/entw-infoaustausch-terrorbek.pdf;jsessionid=8F0CDB27679238C6F4A52F3143693585.2_cid287?__blob=publicationFile, *archived at* http://perma.cc/2WPG-4GV8.

[9] Act on the Federal Office for the Protection of the Constitution § 2, para. 1.

[10] *Id.* § 1, para. 1.

[11] *Id.* § 1, para. 2.

[12] FEDERAL MINISTRY OF THE INTERIOR, 2014 ANNUAL REPORT ON THE PROTECTION OF THE CONSTITUTION. FACTS AND TRENDS, https://www.verfassungsschutz.de/embed/annual-report-2014-summary.pdf, *archived at* http://perma.cc/XTU5-BKUR.

- efforts
    - directed against the free democratic order; or
    - threatening the existence or the security of the federation or one of its states; or
    - aimed at unlawfully hampering constitutional bodies of the federation or one of its states or their members in the performance of their duties; or
    - jeopardizing external relations of Germany through the use of violence or preparation thereof; or
    - directed against the idea of international understanding (art. 9, para. 2 of the German Basic Law), in particular against the peaceful coexistence of nations (art. 26, para. 1 of the German Basic Law); or concerning
- activities threatening national security or intelligence activities carried out on behalf of a foreign power (counterintelligence).

In addition, the agencies for the protection of the constitution participate in security vetting procedures for persons working in sensitive areas.[13]

When the requirements of section 3 of the Act on the Federal Office for the Protection of the Constitution are fulfilled, the agency may use confidential informants, surveillance, telecommunications surveillance, image and sound recordings, false documents, and false vehicle license plates in order to gather intelligence.[14] It may also request information from postal or telecommunication services, financial institutions, airlines, and Internet service providers.[15]

B. Military Counter-Intelligence Service (MAD)

The MAD forms part of the Federal Ministry of Defense. Its purpose and tasks are similar to the BfV, but with the difference that it focuses on efforts and activities that target personnel, departments, or facilities of the Federal Ministry of Defense and are carried out by individuals who are members of, or are employed by the ministry of defense and its agencies.[16] Section 3 of the Military Counter-Intelligence Service Act provides that the BfV and the MAD are required to cooperate closely and to provide mutual support and assistance.

Even though the MAD generally focuses on gathering domestic intelligence, as an exception, it is also authorized to collect and analyze information during the course of special foreign

[13] Act on the Federal Office for the Protection of the Constitution, § 3, para. 2; Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes [Sicherheitsüberprüfungsgesetz] [SÜG] [Security Screening Act], Apr. 20, 1994, BGBL. I at 867, as amended, § 3, paras. 2, 3, http://www.gesetze-im-internet.de/bundesrecht/s_g/gesamt.pdf, *archived at* http://perma.cc/3GBJ-JVU5.

[14] Act on the Federal Office for the Protection of the Constitution §§ 8, 9.

[15] *Id*. § 8a.

[16] Act on the Military Counter-Intelligence Service § 1.

assignments of the German Federal Armed Forces or during the course of humanitarian missions.[17] Other foreign intelligence gathering is prohibited.[18]

C. Federal Intelligence Service (BND)

The BND reports directly to the federal chancellery and is generally the only intelligence agency authorized to gather foreign intelligence.[19] For this purpose, it collects and analyzes information that is of importance for German foreign and security policy.[20] It is also authorized to request information from postal or telecommunication services, financial institutions, airlines, and Internet service providers, as well as information required for the performance of its functions, including personal data, from every authority, and to inspect official registers.[21]

The intelligence objectives of the BND are defined by the mission statement of the federal government. The mission statement currently focuses on proliferation, international terrorism, failing states, and conflicts over natural resources. Regions that it currently prioritizes are the Near and Middle East, North Africa, and West and Central Asia.[22]

III. Legislative Framework

The work of the intelligence agencies is undertaken in accordance with the legislative framework of the Act on the Federal Office for the Protection of the Constitution, the Act on the Military Counter-Intelligence Service, the Act on the Federal Intelligence Service, and the Act to Restrict the Privacy of Correspondence, Mail, and Telecommunications (Article 10 Act).[23]

For law enforcement and police agencies, authorizations are contained in the Act on the Federal Criminal Police Office, the Act on the Federal Police, the Act on the Customs Investigation Bureau and the Customs Investigation Offices, and the Code of Criminal Procedure.[24]

---

[17] *Id.* § 14.

[18] *Id.* § 14, para. 1, sentence 3.

[19] Act on the Federal Intelligence Service §§ 1, 12.

[20] *Id.*

[21] *Id.* § 2a, § 8, para. 3.

[22] *Auftragsprofil der Bundesregierung* [*Mission Statement of the Federal Government*], BUNDESNACHRICHTENDIENST [FEDERAL INTELLIGENCE SERVICE], http://www.bnd.bund.de/DE/Auftrag/Aufgaben/Auftragsprofil_der_Bundesregierung/Auftragsprofil_node.html (last visited June 3, 2016), *archived at* http://perma.cc/72PM-73VV.

[23] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses [Artikel 10-Gesetz] [G 10] [Act to Restrict the Privacy of Correspondence, Mail, and Telecommunications] [Article 10 Act], June 26, 2001, BGBL. I at 1254, 2298, as amended, http://www.gesetze-im-internet.de/bundesrecht/g10_2001/gesamt.pdf, *archived at* http://perma.cc/6YVZ-UCCU, unofficial English translation *available at* http://www.ennir.be/sites/default/files/pictures/GermanLawsgoverningParliamentaryControlofIntelligenceActivities.pdf, *archived at* http://perma.cc/9VKD-LDJH.

[24] STRAFPROZESSORDNUNG [STPO] [CODE OF CRIMINAL PROCEDURE], Apr. 7, 1987, BGBL. I at 1074, 1319, as amended, §§ 100a-100j, http://www.gesetze-im-internet.de/bundesrecht/stpo/gesamt.pdf, *archived at* http://perma.cc/ZA7K-47GY, unofficial English translation *at* http://www.gesetze-im-internet.de/englisch_

IV. Interception and Transmission of Communications

Article 10 of the German Basic Law provides that the privacy of correspondence, mail, and telecommunications is inviolable. Restrictions may only be imposed pursuant to law. If the restriction serves to protect the free, democratic order or the existence or security of the German federation or of a German state, the law may provide that the affected person will not be informed of the measure.

The abovementioned German intelligence and law enforcement agencies have been authorized to access, intercept, and request stored communications data. This authority and its limits are delineated in article 10 of the Basic Law as noted above, in the specific acts establishing the agencies, in the Article 10 Act, and in the Telecommunications Act.[25]

The German Federal Constitutional Court has held that the transmission of subscriber data by telecommunications providers to a requesting agency is only permissible if there is a legal norm authorizing the agency to request the data and an additional legal norm obligating the telecommunications provider to transfer the data ("double door model").[26] If the agency is authorized by law to request communications data, the Telecommunications Act requires telecommunications providers to immediately comply with such a request. "Telecommunications providers" are defined as anyone who exclusively or occasionally provides telecommunications services or who contributes to the provision of such services.[27]

Anyone who operates a telecommunications network that provides publicly available telecommunications services to more than ten thousand participants is obligated to install a surveillance system that complies with the technical requirements set out in the Telecommunications Surveillance Directive and the technical guideline adopted by the German Federal Network Agency.[28] Telecommunications providers must ensure that they are at all times

---

stpo/german_code_of_criminal_procedure.pdf, *archived at* http://perma.cc/8PSW-G87S. (English translation only current up to 2014).

[25] Telekommunikationsgesetz [TKG] [Telecommunications Act], June 22, 2004, BGBL. I at 1190, as amended, §§ 110–115, http://www.gesetze-im-internet.de/bundesrecht/tkg_2004/gesamt.pdf, *archived at* http://perma.cc/WP2Y-XH69.

[26] BUNDESVERFASSUNGSGERICHT [BVERFG] [FEDERAL CONSTITUTIONAL COURT], 100 ENTSCHEIDUNGEN DES BUNDESVERFASSUNGSGERICHTS [BVERFGE] [DECISIONS OF THE FEDERAL CONSTITUTIONAL COURT] 313, 366 *et seq.*, http://www.bundesverfassungsgericht.de/ SharedDocs/Entscheidungen/EN/1999/07/rs19990714_1bvr 222694en.html, *archived at* http://perma.cc/QBZ9-3B9A.

[27] Telecommunications Act, § 3, no. 6.

[28] Telekommunikations-Überwachungsverordnung [TKÜV] [Telecommunications Surveillance Directive], Nov. 3, 2005, BGBL. I at 3136, as amended, §§ 3, 5, para. 1, http://www.gesetze-im-internet.de/bundesrecht/tk_v_2005/ gesamt.pdf, *archived at* http://perma.cc/4MFL-9LW8; Technical Guideline for the Implementation of Legal Measures for the Surveillance of Telecommunications and the Disclosure of Information, Oct. 15, 2015, http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/TechnUmsetzung110/Downloads/TRTK%C3%9CV%20englische%20Version.pdf?__blob=publicationFile&v=7, *archived at* http://perma.cc/F382-S4TE.

capable of being informed by telephone of incoming requests and their urgency, and that they are able to accept and process such requests during regular business hours.[29]

V. Oversight

The intelligence agencies are subject to administrative as well as parliamentary oversight. There are several specialized parliamentary control panels that were set up to scrutinize the work of the intelligence agencies, but they are also subject to the general framework of parliamentary oversight.

A. Parliamentary Oversight

1. Parliamentary Control Panel (PKGr)

Article 45d of the German Basic Law provides that the German Parliament must appoint a panel to scrutinize the federal intelligence activities. Based on this constitutional provision, the Parliament enacted the Act on the Parliamentary Control of the Intelligence Activities of the Federation, which established the Parliamentary Control Panel (PKGr).[30] The PKGr oversees the Federal Office for the Protection of the Constitution, the Military Counter-Intelligence Service, and the Federal Intelligence Service.

The members of the PKGr are appointed by the Parliament from among their members; the Parliament also decides the number of members, the composition, and the PKGr's working methods.[31] The Parliamentary Control Panel currently has nine members.[32] The deliberations of the PKGr are conducted in secret.[33]

The federal government is required to disclose comprehensive information on the general activities of the federal intelligence services and of activities of particular importance to the Panel, as well as on other procedures if requested by the PKGr.[34] Furthermore, the PKGr may require the federal government and the federal intelligence agencies to release files and other documents in official safekeeping and to transmit data stored in data files. It may also obtain access to all official premises and interview members of the intelligence services and the federal

---

[29] Telecommunications Surveillance Directive § 12.

[30] Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes [Kontrollgremiumgesetz] [PKGrG] [Act on the Parliamentary Control of the Intelligence Activities of the Federation] [Parliamentary Control Panel Act], July 29, 2009, BGBL. I at 2346, as amended, http://www.gesetze-im-internet.de/bundesrecht/pkgrg/gesamt.pdf, *archived at* http://perma.cc/2ZCX-LUS4, unofficial English translation *available at* http://www.ennir.be/sites/default/files/pictures/GermanLawsgoverningParliamentaryControlof IntelligenceActivities.pdf, *archived at* http://perma.cc/9VKD-LDJH.

[31] Parliamentary Control Panel Act § 2.

[32] *Mitglieder des Parlamentarischen Kontrollgremiums (PKGr)* [*Members of the Parliamentary Control Panel (PKGr)*], DEUTSCHER BUNDESTAG [GERMAN PARLIAMENT], http://www.bundestag.de/bundestag/gremien18/pkgr/mitglieder/261126 (last visited June 3, 2016), *archived at* http://perma.cc/GN62-WFLQ.

[33] *Id.* § 10.

[34] Parliamentary Control Panel Act § 4.

government. The courts and public authorities are required to provide legal and administrative assistance.[35]

In addition, the Act on the Federal Office for the Protection of the Constitution,[36] the Act on the Military Counter-Intelligence Service,[37] and the Article 10 Act[38] also contain special notification requirements.

The PKGr reports to the German Parliament on its oversight activities halfway through and at the end of each electoral term.[39] The reports are publicly available in the Parliamentary Material Information System (DIP).[40]

2. Article 10 Commission

Restrictions on the privacy of mail and telecommunications undertaken by the federal intelligence agencies pursuant to article 10 of the German Basic Law are monitored by the Article 10 Commission.[41] The Article 10 Commission is appointed by the Parliamentary Control Panel and is composed of four members. The chairperson must be qualified to hold judicial office. In addition, there are four alternate members who may take part in the meetings with the right to speak and to ask questions.[42]

The G10 Commission decides ex officio or on the basis of complaints whether restrictions on the privacy of mail and telecommunications are permissible and necessary. The oversight extends to the entire scope of collecting, processing, and using the personal data obtained pursuant to the Article 10 Act by the federal intelligence agencies.[43]

Before a restriction on the privacy of mail and telecommunications can be enforced, the federal ministry in charge has the obligation to report every month to the Article 10 Commission and to request approval. In cases of imminent danger, a restriction may be enforced without prior approval. Approval must be obtained without undue delay.[44]

---

[35] *Id.* § 5.

[36] Act on the Federal Office for the Protection of the Constitution § 8a, para. 6.

[37] Act on the Military Counter-Intelligence Service § 14, paras. 6, 7.

[38] Article 10 Act § 14.

[39] Parliamentary Control Panel Act § 13.

[40] The latest report for the period between November 2013 and December 2015 was published in March 2016. *See* DEUTSCHER BUNDESTAG: DRUCKSACHEN UND PROTOKOLLE [BT-DRS.] 18/7962, http://dipbt.bundestag.de/doc/btd/18/079/1807962.pdf, *archived at* http://perma.cc/LU7G-PCS7.

[41] Article 10 Act § 1, para. 2, § 15.

[42] *Id.* § 15.

[43] *Id.* § 15, para. 5.

[44] *Id*. § 15, para. 6.

3. Confidential Committee of the Budget Committee

The operating budgets of the federal intelligence agencies are not submitted to the general budget committee, but approved by a special committee called the Confidential Committee of the Budget Committee, which works under conditions of secrecy.[45] The members are elected by the German Parliament according to the process used for the election of the members of the PKGr. The Federal Budget Code provides that the Confidential Committee of the Budget Committee has the same control rights as the PKGr laid down in sections 5, 6, 7, 8, 12, and 13 of the Parliamentary Control Panel Act.[46] These rights include access to files and data stored in data files, access to all official premises, and the right to interview members of the intelligence services and the federal government.

The PKGr and the Confidential Committee are obligated to consult with and advise each other in order to avoid oversight gaps.[47]

4. General Parliamentary Oversight

In addition, the work of the federal intelligence agencies is subject to general parliamentary oversight.[48] This includes responding to requests from committees of inquiry[49] and other specialized committees, answering questions in general debates and in debates on matters of topical interest,[50] and answering formalized requests (interpellations) from minority groupings and individual members of Parliament.[51] The Federal Constitutional Court has held that communications concerning contacts with foreign intelligence services cannot be withheld from a committee of inquiry by generally invoking the interests of the state; instead, specific reasons must be given.[52]

B. Administrative Oversight

1. Administrative and Technical Supervision by Competent Federal Ministry

The Federal Chancellery as well as the Federal Ministry of the Interior and the Federal Ministry of Defense are authorized to request statements and issue instructions for the respective intelligence agency under their supervision.

---

[45] BUNDESHAUSHALTSORDNUNG [FEDERAL BUDGET CODE], Aug. 19, 1969, BGBl. I at 1284, as amended, § 10a, para. 2, http://www.gesetze-im-internet.de/bundesrecht/bho/gesamt.pdf, *archived at* http://perma.cc/Y8Y8-G6J4.

[46] FEDERAL BUDGET CODE § 10a, para. 2.

[47] Parliamentary Control Panel Act § 9, para. 1.

[48] *Id*. § 1, para. 2.

[49] Basic Law art. 44.

[50] *Id.* art. 43, para. 1.

[51] *Id.* art. 38, para. 1, sentence 2, art. 20, para. 2, sentence 2.

[52] BVerfG, 124 BVerfGE 78, 123 et seq., press release summarizing the decision in English *available at* https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2009/bvg09-084.html, *archived at* http://perma.cc/7JJW-SCUC.

2. Federal Commissioner for Data Protection and Freedom of Information

The Federal Commissioner for Data Protection and Freedom of Information monitors compliance of the federal intelligent agencies with data protection laws, in particular the Federal Data Protection Act,[53] but also with the special data provisions contained in the acts establishing the federal intelligence agencies.[54] The Commissioner has no powers with regard to data collected through mail and telecommunications surveillance. In these cases, responsibility lies solely with the Article 10 Commission.

The Commissioner is appointed by the German Parliament on a proposal from the federal government for a five-year term.[55] He or she is independent in the discharge of his or her duties and subject only to the law.[56]

3. Federal Court of Audit

The Federal Court of Audit determines if public finances have been properly spent and efficiently administered. A body called the "College of Three" composed of the president or vice president of the Court of Audit, the head of the unit, and the responsible audit director is in charge of the audit of the federal intelligence agencies' budgets.[57] The College of Three informs the Confidential Committee of the Budget Committee, the PKGr, the federal ministry supervising the intelligence agency, and the Federal Ministry of Finance about the results of the audit of the annual account and the budgetary and economic management of the respective federal intelligence agency.[58]

---

[53] Bundesdatenschutzgesetz [Federal Data Protection Act], Jan. 14, 2003, BGBL. I at 66, as amended, http://www.gesetze-im-internet.de/bundesrecht/bdsg_1990/gesamt.pdf, *archived at* http://perma.cc/5AH5-8YT2, unofficial English translation *available at* http://www.gesetze-im-internet.de/englisch_bdsg/federal_data_protection_act.pdf, *archived at* http://perma.cc/AD3N-DPY3.

[54] Federal Act on Protection of the Constitution §§ 14, 15, 22a; Act on the Federal Intelligence Service §§ 2, 9a, 10.

[55] Federal Data Protection Act § 22.

[56] *Id.* § 22, para. 4.

[57] Gesetz über den Bundesrechnungshof (Bundesrechnungshofgesetz – BRHG) [Act on the Federal Court of Audit], July 11, 1985, BGBL. I at 1445, as amended, §§ 9, 19, https://www.gesetze-im-internet.de/bundesrecht/brhg_1985/gesamt.pdf, *archived at* http://perma.cc/23VP-M2YP.

[58] Federal Budget Code § 10a, para. 3.

Portugal

Eduardo Soares
Senior Foreign Law Specialist

SUMMARY Constitutional principles guarantee the protection of personal data in Portugal, including its collection and use, and the privacy of a person's home and communications. An information system composed of intelligence services and supervisory bodies is in charge of producing intelligence for the purpose of defending national interests. European Union Directives have been transposed into the country's domestic legal system to regulate the protection of personal data and privacy in the telecommunications and electronic communications sectors.

I. Constitutional Principles

The protection of personal data used in connection with information technology is a fundamental right guaranteed by the Portuguese Constitution of 1976.[1] The law must establish effective guarantees against the acquisition and abusive use, or use that is contrary to human dignity, of information concerning individuals and families.[2] The home and the privacy of correspondence and other private means of communication are inviolable.[3] Any interference by public authorities with correspondence, telecommunications, or other means of communication is prohibited, except in cases provided by law on matters of criminal procedure.[4]

II. Information System of the Portuguese Republic

In Portugal, intelligence activities are coordinated by the Information System of the Portuguese Republic (Sistema de Informações da República Portuguesa, SIRP). Law No. 30 of September 5, 1984, establishes the general basis of SIRP.[5] The purposes of SIRP are reflected exclusively in the powers and prerogatives of the information services provided for in Law No. 30.[6] These information services are responsible for ensuring, in compliance with the Constitution and the law, the production of information necessary for the preservation of internal and external security, as well as the independence and national interests, unity, and integrity of the state.[7]

---

[1] CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA (Constitutional Revision VII (2005)) art. 35, http://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx, *archived at* https://perma.cc/359T-WEA7.

[2] *Id.* art. 26(2).

[3] *Id.* art. 34(1).

[4] *Id.* art. 34(4).

[5] Lei No. 30/84, de 5 de Setembro, *as amended by* Lei Orgânica No. 4/2014 [Organic Law No. 4 of Aug. 13, 2014], art. 1, http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=764&tabela=leis, *archived at* https://perma.cc/V8YF-CY26.

[6] *Id.* art. 2(1).

[7] *Id.* art. 2(2).

Among the bodies created to achieve the purposes of Law No. 30 are the Strategic Information Service of Defense (Serviço de Informações Estratégicas de Defesa, SIED)[8] and the Security Information Service (Serviço de Informações de Segurança, SIS).[9] SIED is in charge of producing information that may assist in safeguarding national independence, national interests, and the external security of the country,[10] while SIS is in charge of producing information to assist in safeguarding internal security and the prevention of sabotage; terrorism; espionage; and the performance of acts that, by their nature, may alter or destroy the state as constitutionally established.[11]

Law No. 30 determines that activities that involve researching, processing, and disseminating information that poses a threat or violates the rights, freedoms, and guarantees embedded in the Constitution and the law cannot be carried out.[12] Accordingly, the information services are subject to all the restrictions established by law in defense of rights and freedoms.[13] Each information service may develop research activities and process information related only to its specific mission, without prejudice to the obligation to mutually communicate data and information that may be relevant to the achievement of SIRP's purposes.[14]

Civil or military employees or agents of the information services provided for in Law No. 30 are not authorized to exercise powers, perform actions, or carry out activities under the specific jurisdiction of the courts and bodies with police functions.[15] The information services may have data centers consistent with the nature of the service, which must process and save on magnetic files the data and information collected in the course of their business.[16] Each data center works autonomously and is not permitted to be connected with other data centers.[17]

III. European Union Directives and Domestic Laws

In 1995, the European Union issued Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.[18] During

[8] *Id.* art. 7(e).

[9] *Id.* art. 7(f).

[10] *Id.* art. 20; *see also* Lei No. 9/2007, de 19 Fevereiro [Law No. 9 of Feb. 19, 2007], *as amended by* Lei No. 50/2014 [Law No. 50 of Aug. 13 of 2014], art. 26, http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=910&tabela=leis&ficha=1&pagina=1&, *archived at* https://perma.cc/LQ9L-HXDV.

[11] Lei No. 30/84, art. 21; *see also* Lei No. 9/2007, art. 33.

[12] Lei No. 30/84, art. 3(1).

[13] *Id.* art. 3(2).

[14] *Id.* art. 3(3).

[15] *Id.* art. 4(1).

[16] *Id.* art. 23(1); *see also* Lei No. 9/2007, arts. 41–43.

[17] Lei No. 30/84, art. 23(2).

[18] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML, *archived at*

Portugal's Constitutional Review of 1997, article 35 of the Constitution was amended to enable an adequate transposition of Directive No. 95/46/EC into Portugal's Constitutional Charter.[19] Subsequently, Law No. 67 of October 26, 1998, which transposed Directive No. 95/46/EC into Portugal's domestic legislation, was enacted as the new law on the protection of personal data.[20]

Law No. 41 of August 18, 2004, transposed Directive 2002/58/EC on Privacy and Electronic Communications into Portugal's domestic legislation.[21] Law No. 41 applies to the processing of personal data in the context of networks and electronic communication services available to the public, specifying and supplementing the provisions of Law No. 67/98.[22]

The processing of personal data referring to philosophical or political beliefs, political party or union membership, religious faith, private life, and racial or ethnic origin, as well as the processing of data concerning a person's health or sex life, including genetic data, is prohibited under article 7(1) of Law No. 67/98.[23] However, article 7(2) of Law 67/98 determines that the processing of the data mentioned in article 7(1) is allowed if permission is provided by law or authorized, in specific situations, by the National Commission of Data Protection (Comissão Nacional de Protecção de Dados, CNPD).[24] Article 5(1) of Law No. 67/98 lists the requirements for the collection and treatment of personal data.[25]

On July 17, 2008, Law No. 32 was issued to regulate the storage and transmission of traffic and location data relative to natural persons and legal entities, as well as the related data necessary to identify the subscriber or registered user, for purposes of the investigation, detection, and prosecution of serious crimes by the competent authorities.[26] Law No. 32 transposed Directive

---

https://perma.cc/GG7B-VDK9 (click "See the Screenshot View"). For a discussion of this and other EU legislation, see EU survey.

[19] QUARTA REVISÃO CONSTITUCIONAL, Lei Constitucional No. 1/97, de 20 de Setembro, art. 18, http://www.pgdlisboa.pt/pgdl/leis/lei_mostra_articulado.php?nid=11&tabela=leis&ficha=1&pagina=1, *archived at* https://perma.cc/UT7S-YX96.

[20] Lei No. 67/98, de 26 de Outubro, Lei da Protecção de Dados Pessoais [Personal Data Protection Law], http://www.pgdlisboa.pt/pgdl/leis/lei_mostra_articulado.php?nid=156&tabela=leis&ficha=1&pagina=1, *archived at* https://perma.cc/4Y92-FX9K.

[21] Lei No. 41/2004, de 18 de Agosto, http://www.pgdlisboa.pt/pgdl/leis/lei_mostra_articulado.php?nid=707&tabela=leis&ficha=1&pagina=1, *archived at* https://perma.cc/Q28H-4DF4; Directive 2002/58/EC, of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), 2002 O.J. (L 201) 37, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML, *archived at* https://perma.cc/BRG6-HTXK (click "See the Screenshot View").

[22] Lei No. 41/2004, art. 1(2).

[23] Lei No. 67/98, art. 7(1).

[24] *Id.* art. 7(2). Article 22(1) of Law No. 67/98 determines that the CNPD is the national authority charged with the power to supervise and monitor compliance with the laws and regulations in the area of personal data protection, with strict respect for human rights and fundamental freedoms, and the guarantees provided by the Constitution and the law.

[25] *Id.* art. 5(1).

[26] Lei No. 32/2008, de 17 de Julho, art. 1(1), http://www.pgdlisboa.pt/pgdl/leis/lei_mostra_articulado.php?nid=1264&tabela=leis&ficha=1&pagina=1&, *archived at* https://perma.cc/8R6E-KM4U.

2006/24/EC into Portugal's domestic legal system.[27] According to Law No. 32, the retention of data revealing the content of communications is prohibited, without prejudice to the provisions of Law No. 41/2004 and criminal procedure law on the interception and recording of communications.[28]

The storage and transmission of data must be made exclusively in connection with the investigation, detection, and prosecution of serious crimes by the competent authorities.[29] The transmission of data to the competent authorities may be authorized only by a written order issued by a judge, in accordance with article 9 of Law No. 32/2008.[30] The files for the retention of data under Law No. 32/2008 must be separated from any other files used for other purposes.[31] The data subject cannot oppose the storage and transmission of data.[32]

[27] Directive 2006/24/EC, of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 54, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0024, *archived at* https://perma.cc/A28Q-XFJ8 (click "See the Screenshot View").

[28] Lei No. 32/2008, art. 1(2).

[29] *Id.* art. 3(1).

[30] *Id.* art. 3(2).

[31] *Id.* art. 3(3).

[32] *Id.* art. 3(4).

Romania

Nerses Isajanyan
Foreign Law Consultant

SUMMARY Intelligence gathering in Romania is divided among several government agencies as provided in national security legislation. Constitutional principles guarantee the protection of privacy and personal data. Surveillance and intelligence gathering is conducted in accordance with national criminal procedural legislation. Control over intelligence activities by government agencies is exerted legislatively by the Parliament and through the judicial review of warrants for data collection issued by prosecutorial offices. The latter form of control, however, appears to be inefficient due to judicial weakness.

I. Introduction

The Romanian intelligence community consists of the following services and ministerial substructures charged with intelligence collection:

- Domestic Intelligence Service (Serviciul Român de Informații, SRI)
- Foreign Intelligence Service (Serviciul de Informații Externe, SIE)
- Guard and Protection Service (Serviciul de Protecţie şi Pază, SPP, in charge of protecting Romanian and foreign VIPs)
- Defense Ministry's Directorate of Defense Intelligence
- Interior Ministry's General Directorate of Intelligence and Internal Protection (police)
- Justice Ministry's special units[1]

Each agency works in a specific field within the scope of its jurisdiction as assigned by the Law on National Security of Romania.[2] The SIE was created under a specific law that defined its duties and created a multilayered oversight structure aimed at immunizing the Service from political manipulations along party lines.[3] The Service operates independently of the government and is not subordinate to the incumbent executive.[4] The Law states that the means

[1] HANS BORN & MARINA CAPARINI, DEMOCRATIC CONTROL OF INTELLIGENCE SERVICES: CONTAINING ROGUE ELEPHANTS 48 (Ashgate Pub. 2013).

[2] Law No. 51/1991 on National Security of Romania, MONITORUL OFFICIAL [MO] [OFFICIAL GAZETTE], Aug. 7, 1991, English translation *available at* https://www.sri.ro/fisiere/legislation/Law_national-security.pdf, *archived at* https://perma.cc/2VCU-HNEA.

[3] Law No. 1/1998 on the Organization and Functioning of the Foreign Intelligence Service, MO, Jan. 6, 1998, https://www.sie.ro/legislatie_Legea_nr.1-1998.html (in Romanian), *archived at* https://perma.cc/JWJ7-96QP.

[4] COUNCIL OF EUROPE, CIA ABOVE THE LAW? SECRET DETENTIONS AND UNLAWFUL INTER-STATE TRANSFERS OF DETAINEES IN EUROPE 201 (2008).

of intelligence gathering must not violate citizens' basic rights and freedoms, private life, or honor and reputation, nor can it impose on them any illegal restraints.[5]

To ensure the unified coordination of all activities pertaining to defense and state security, including intelligence operations, the National Defense Supreme Council, an autonomous administrative body managed by the Office of the President of Romania, was created by law in 1990.[6] Additionally, the Council coordinates and monitors activities of the SRI, SEI, and SPP.[7]

On February 16, 2016, the Constitutional Court of Romania issued an important decision that affected the structure and competences of intelligence agencies.[8] Interpreting a provision of the Criminal Procedure Code on technical surveillance, the Court concluded that intelligence collected through wiretapping and other technical means is inadmissible as evidence if it was not obtained by the police or a criminal investigation body.[9] This decision directly affected the SRI because it was not considered a criminal investigative body. The director of the SRI even stated that the decision impacted national security and that the SRI's technical surveillance department had become useless.[10] The decision could impact thousands of ongoing corruption and organized crime investigations and cases already pending in court.[11]

Before the Court's ruling, the SRI had conducted technical surveillance at the request of the prosecutor's office and other agencies in cases involving not only national security but also corruption, tax evasion, and other crimes.[12] The SRI was also the only agency with sufficient technical capacity to conduct such surveillance. According to a European news source, "the system contains very few checks and balances. Nobody really knows if the [SRI] is controlling in any way the flow of information, deciding what to give away and what to hold back."[13]

---

[5] Law No. 1/1998 on the Organization and Functioning of the Foreign Intelligence Service art. 10(3).

[6] Law No. 39/1990 on the Setting Up, Organization and Functioning of the Supreme Council of National Defense, MO, Dec. 13, 1990, *repealed by* Law No. 415/2002 on the Organization and Functioning of the Supreme Council of National Defense, MO, July 10, 2002, https://www.sie.ro/legislatie_Legea_nr.415-2002.html (in Romanian), *archived at* https://perma.cc/GH7B-D2D4.

[7] THOMAS BRUNEAU & STEVEN BORAZ, REFORMING INTELLIGENCE: OBSTACLES TO DEMOCRATIC CONTROL AND EFFECTIVENESS 255 (U. Tex. Press 2009).

[8] Decision of the Constitutional Court No. 51 of Feb. 16, 2016, English translation *available at* https://www.ccr.ro/files/products/Decizie_51_2016_ENG.pdf, *archived at* https://perma.cc/59W8-ZG8S.

[9] Irina Popescu, *Romanian Intelligence Service Wiretapping Is Unconstitutional, Court Rules*, ROMANIA-INSIDER.COM (Feb. 18, 2016), http://www.romania-insider.com/romanian-intelligence-service-wiretapping-is-unconstitutional-court-rules, *archived at* https://perma.cc/9BRL-KA42.

[10] *Romania's Govt. Grants Investigation Powers to the Biggest Secret Service, Sets Rules for Wiretaps*, ROMANIA-INSIDER.COM (Mar. 13, 2016), http://www.romania-insider.com/romanias-government-grants-more-powers-to-the-biggest-secret-service-sets-rules-for-wiretaps/166785, *archived at* https://perma.cc/V7ZX-NA8L.

[11] *Wiretaps Deemed Unconstitutional in 11 Corruption Cases in Romania*, ROMANIA-INSIDER.COM (Mar. 11, 2016), http://www.romania-insider.com/wiretaps-deemed-unconstitutional-in-11-corruption-cases-in-romania/166698, *archived at* https://perma.cc/PWV4-9C79.

[12] *Romania's Govt. Grants Investigation Powers to the Biggest Secret Service*, *supra* note 10.

[13] Vlad Stoicescu, *Understanding Romania's Anitcorruption Hunt*, KATOIKOS.EU (Apr. 8, 2015), http://www.katoikos.eu/opinion/understanding-romanias-anticorruption-hunt.html, *archived at* https://perma.cc/A732-BRUH.

Following the decision of the Constitutional Court, President Iohannis stated that an emergency ordinance would be adopted by the government as a temporary solution to the problem.[14] The ordinance, adopted on March 11, 2016,[15] granted criminal investigative powers to the SRI in cases involving terrorism and crimes against national security. Previously, the SRI could only notify the prosecutors of such crimes and assist with the investigation.

In addition, the emergency ordinance gave wiretapping powers to the National Anticorruption Directorate (Directia Nationala Anticoruptie, DNA) at the State Prosecutor's Office within the High Court, and the Directorate for Investigating Organized Crime and Terrorism at the National Police (Directia de Investigare a Infractiunilor de Criminalitate Organizata si Terorism, DIICOT). Before the Constitutional Court's decision these bodies mostly used SRI personnel and equipment for technical surveillance. Now they can still use the SRI's equipment but not its personnel.[16] Reportedly DNA's technical center would increase its staff by 130 officers while the Prosecutor's Office and the DIICOT would employ three hundred officers.[17]

Making the SRI a criminal investigation body was criticized by legal professionals and civil society, as it legalizes the involvement of a secret intelligence agency in the judicial process, undermining the SRI's independence,[18] and "brings back terrifying memories of Ceausescu's Securitate."[19]

II. Legislative Oversight

The SIE and the SRI are subject to parliamentary control through special parliamentary committees individually dedicated to each agency.[20] These committees consist of nine members each, seven representing the lower chamber of the Parliament and two representing the Senate.[21]

---

[14] Daniela Budu, *The Romanian Intelligence Service and Technical Surveillance*, RADIO ROMANIA INTERNATIONAL (Mar. 14, 2016), http://www.rri.ro/en_gb/the_romanian_intelligence_service_and_technical_surveillance-2544757, *archived at* https://perma.cc/NS7M-DVDR.

[15] Emergency Ordinance No. 6 of March 11, 2016, MO, Mar. 14, 2016, *available at* http://lege5.ro/Gratuit/geydcmrwgi2q/ordonanta-de-urgenta-nr-6-2016-privind-unele-masuri-pentru-punerea-in-executare-a-mandatelor-de-supraveghere-tehnica-dispuse-in-procesul-penal (in Romanian), *archived at* https://perma.cc/4H2E-Y3TY.

[16] *Romania's Govt. Grants Investigation Powers to the Biggest Secret Service*, *supra* note 10.

[17] *How Many Interception Centers Are in Romania? Who Are the Institutions Taping Our Calls*, ANTENA3.RO (Mar. 15, 2016), http://www.antena3.ro/en/romania/how-many-interception-centers-are-in-romania-who-are-the-institutions-taping-our-calls-346350.html, *archived at* https://perma.cc/2U4X-4FVE.

[18] *Is Europe Under Siege? MEDEL Declaration*, MEDEL (Mar. 12, 2016), http://www.medelnet.eu/index.php?option=com_content&view=article&id=240:is-europe-under-siege-medel-declaration&catid=45:an-independent-judiciary&Itemid=61, *archived at* https://perma.cc/4TG2-ACK3.

[19] Bogdan Manolea, ApTI, *Intelligence Organisations Get More Surveillance Powers in Romania*, EDRI (Apr. 6, 2016), https://edri.org/intelligence-organisations-get-more-surveillance-powers-in-romania, *archived at* https://perma.cc/DVE9-SHHZ.

[20] COUNCIL OF EUROPE, *supra* note 4, at 201.

[21] Rule No. 44/1998 on the Setting Up, Organization and Functioning of the Special Parliamentary Commission for Overseeing the Foreign Intelligence Service, https://www.sie.ro/legislatie_Hotararea_nr.44-1998.html, *archived at* https://perma.cc/4VL7-3EAX.

Each party represented in Parliament has members on these committees.[22] Both committees overseeing the SRI and SIE are empowered to verify constitutional and legal compliance of the Services' activities and investigate allegations of illegal intelligence collection.[23]

The committees are allowed to request information possessed by the SRI and SIE. Both Services are required to respond to such requests within a reasonable period of time, unless doing so jeopardizes ongoing operations, the identities of agents, or intelligence sources and methods.[24] The committees are authorized to investigate the directors of the agencies and their staff members and have the right to conduct unannounced visits to the Services, which must grant the committees full access to personnel, data, and facilities.[25] Reportedly the committees have uncovered corruption and links to organized crime within the agencies, and violations of civil rights and liberties committed by intelligence services personnel.[26] On the basis of media accusations, parliamentary committees initiated a series of SRI and SIE investigations and inquiries, which resulted in the removal of personnel.[27] For example, in May 2016 the committee controlling the activities of the SRI initiated an inquiry into the investigation of a local pharmaceutical company, Hexi Pharma, which sold diluted disinfectants to local hospitals. The committee will try to determine if the SRI was involved in the criminal investigation against Hexi Pharma and if the case was classified as a national security case.[28]

III. Judicial Control over Surveillance Procedures

Judicial oversight is generally limited to the consideration and issuance of warrants for surveillance that restrict an individual's civil rights and liberties.[29] The National Security Law authorized the SRI and SIE to undertake intelligence surveillance and established preemptive control by judicial authorities.[30] Article 13 of the Law states that requests for warrants must be approved by the Prosecutor General's office and must contain details regarding the following:

- Nature of the threat to national security
- Specific activities for which the warrant is being issued (e.g., surveillance, wiretapping, search, seizure)

[22] BRUNEAU & BORAZ, *supra* note 7, at 227.

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.* at 233.

[28] *Parliamentary Committee to Check Romanian Secret Service in Disinfectants Case*, ROMANIA-INSIDER.COM (May 24, 2016), http://www.romania-insider.com/parliamentary-committee-check-romanian-secret-service-disinfectants-case, *archived at* https://perma.cc/Z6DF-AUTW.

[29] BORN & CAPARINI, *supra* note 1, at 59.

[30] Law No. 51/1991, arts. 8, 13.

- Names of persons whose communications are to be intercepted, or of those who hold the information, documents, or objects that must be obtained
- Location where the warranted activities will be carried out, if and when it is possible to provide this information
- Duration for which the requested warrant is valid (up to six months initially)
- Office charged with the execution of the warrant[31]

Warrants are valid for six months, although they can be extended an indefinite number of times for three-month periods when cause is shown.[32] In 2005 warrant approval was reassigned from prosecutors to judges, although prosecutors are still permitted to approve short-term (twenty-four- to forty-eight-hour) warrants during weekends when judges are off duty.[33]

The weakness and vulnerability to political influence of the legal and justice system is still a significant obstacle to effective democratic oversight.[34] Government statistics revealed that 14,267 wiretapping warrants were requested between 1989 and 2002 by the intelligence agencies, and the Prosecutor General did not deny a single one.[35] Of the warrants issued, only about 2% led to an indictment, while the intelligence services claimed the remaining 98% were "used for prevention of a crime."[36]

The National Security Law states that "any citizen who considers himself injured in an unjustified manner through the activities that constitute the object of the warrant . . . may lodge a complaint with the public prosecutor specially appointed, hierarchically superior to the public prosecutor who has issued the warrant."[37] The Law provides that citizens who believe that their rights or liberties have been violated by the government in the course of its information gathering have the right to "inform any of the standing comittees [sic] for the defence and ensuring of the public order, of the two chambers of the Parliament."[38]

The emergency ordinance of March 11, 2016, granted criminal investigation powers to the SRI in certain cases involving national security and simultaneously introduced judicial control, which is to be carried out by the chairman of the High Court of Cassation and Justice or a judge appointed for this purpose in accordance with the rules on the operation of the Supreme Court.[39]

---

[31] *Id*. art. 13.

[32] *Id*.

[33] BORN & CAPARINI, *supra* note 1, at 59.

[34] *Id.* at 64.

[35] BRUNEAU & BORAZ, *supra* note 7, at 228.

[36] *Id*.

[37] Law No. 51/1991, art. 13.

[38] *Id.* art. 16.

[39] Mihaela Constantin, *Wiretapping in Romania, Enforced Through Emergency Ordinance*, GOVNET (Mar. 15, 2016), http://govnet.ro/Local/Politics/Wiretapping-Romania-enforced-through-emergency-ordinance-, *archived at* https://perma.cc/7UWN-VXVL.

In 2014 the SRI proposed a new bill that would allow several agencies to gain access to data stored by Internet and phone service providers, without permission from a judge, only on the basis of a "motivated request."[40] The SRI claimed that the law was necessary because of the increasing number of cyber threats.[41] The draft was based on the European Union's (EU's) then-upcoming Network and Information Security Directive, which requires Member States to appoint central authorities in charge of coordinating the response to cyber threats and incidents.[42] However, the final version of the Bill as it was passed by the Romanian legislature in December 2014 ignored the EU recommendation that the authority responsible for cybersecurity be a civilian agency not linked to law enforcement or intelligence.[43] The act was declared unconstitutional in its entirety by the Constitutional Court on January 21, 2015,[44] on various grounds, including those pertaining to the unjustified infringement of the right of individuals to privacy and personal data protection.

The new bill on Romania's cybersecurity was made available for public debate in January 2016,[45] and President Iohannis expected that it would be adopted by the Parliament in June 2016, together with an improved counterterrorism law and a law on prepaid cards.[46] The latter law was prepared at the initiative of the SRI, which complained that it could not keep track of the users of prepaid cards, which were allegedly used in preparing terrorist attacks in the EU.[47]

Regarding terrorism prevention, as of December 2015, the Bucharest Court of Appeal had ordered, on the SRI's recommendation, the removal from the national territory of nine foreigners suspected of terrorist actions, while another 246 persons had been stopped at the border for the

[40] Irina Popescu, *Romanian Constitutional Court: Cyber Security Law Is Unconstitutional*, ROMANIA-INSIDER.COM (Jan. 22, 2015), http://www.romania-insider.com/romanian-constitutional-court-cyber-security-law-is-unconstitutional/140240/-, *archived at* https://perma.cc/7WE4-BQX4.

[41] *Id.*

[42] Lucian Constantin, *Romanian Version of EU Cybersecurity Directive Allows Warrantless Access to Data*, PCWORLD (Dec. 24, 2014), http://www.pcworld.com/article/2863632/romanian-version-of-eu-cybersecurity-directive-allows-warrantless-access-to-data.html, *archived at* https://perma.cc/PMV8-CB5H.

[43] *Id.*

[44] Decision of the Constitutional Court No. 17 of Jan. 21, 2015, English translation *available at* https://www.ccr.ro/files/products/Decizie_17_2015_EN_final.pdf, *archived at* https://perma.cc/3HWW-GLLB.

[45] Adina Panaitescu, *Communications Minister Bostan: I Hope Cybersecurity Law Gets Final Approval from Justice Ministry*, AGERPRES (May 25, 2016), http://www.agerpres.ro/english/2016/05/25/communications-minister-bostan-i-hope-cybersecurity-law-gets-final-approval-from-justice-ministry-13-02-26, *archived at* https://perma.cc/6J8D-RJEN.

[46] Irina Popescu, *Romanian President: Three Laws on National Security to Be Sent to the Parliament by End-May*, ROMANIA-INSIDER.COM (Apr. 13, 2016), http://www.romania-insider.com/romanian-president-three-laws-on-national-security-to-be-sent-to-the-parliament-by-end-may/168740, *archived at* https://perma.cc/Z5TN-GTAT.

[47] Irina Popescu, *Minister: Romania's IT Infrastructure Is Used for Spreading Computer Viruses Worldwide*, ROMANIA-INSIDER.COM (Mar. 28, 2016), http://www.romania-insider.com/romanias-it-infrastucture-is-used-for-spreading-computer-viruses-worldwide/167664, *archived at* https://perma.cc/F4X8-M9S5.

same reasons.[48] According to the director of the agency, the SRI was also monitoring nine thousand other people who do not have access to the national territory.[49]

[48] *Nine Foreigners Suspected of Terrorist Actions Removed from Romania, Other 246 Stopped at Border*, AGERPRES (Dec. 3, 2015), http://www.agerpres.ro/english/2015/12/03/nine-foreigners-suspected-of-terrorist-actions-removed-from-romania-other-246-stopped-at-border-11-10-18, *archived at* https://perma.cc/99ER-3ZPV.

[49] Catalina Mihai, *Romanian President Lauds Intelligence Services, Says Country "Is Safe,"* EURACTIV (Mar. 30, 2016), http://www.euractiv.com/section/security/news/romanian-president-lauds-intelligence-services-says-country-is-safe, *archived at* https://perma.cc/3A6B-TCBN.

Netherlands

Wendy Zeldin
Senior Legal Research Analyst

SUMMARY Foreign intelligence gathering in the Netherlands is regulated chiefly by the Intelligence and Security Services Act 2002. The Act governs both the General Intelligence and Security Service and the Military Intelligence and Security Service, and requires that these Services obtain ministerial permission to exercise most of their powers, such as the power to institute surveillance and wiretaps and use intelligence agents. The Act has come under scrutiny in recent years, however, and there are plans to overhaul it, with expectations that draft legislation may be presented to the Dutch Parliament by the summer of 2016.

I. Introduction

The General Intelligence and Security Service of the Netherlands (Algemene de inlichtingen- en veiligheidsdienst, AIVD), under the Ministry of Internal Affairs and Relations with the Realm, is responsible for investigating individuals and organizations, carrying out security screenings, furthering vital sectors' security, gathering international intelligence, and compiling risk and threat analyses.[1] According to its website, the AIVD seeks to identify risks and threats to Dutch national security by "conducting in-depth investigations to gather intelligence material," which it then "enriches" and shares with various other agencies, in particular the police Regional Intelligence Divisions (RIDs).[2] The AIVD can ask RID personnel to gather intelligence material; it also "works intensively with local governments" to help counter Islamic radicalism.[3] As the AIVD emphasizes on its website, it "is not a police service," and while it "has the access to information, the powers and the expertise" to investigate the roots of national security risks and threats, it does not investigate criminal acts but rather "identifies threats and advises others, including policymakers and public officials at both the national and local levels, as to how they might act upon the information received."[4]

In addition to the police regional intelligence units, there is a Central Intelligence Division that is part of the Central Unit of the National Police.[5] The Central Intelligence Division handles "coordination of law enforcement information in the Netherlands and its exchange at [the] international level" and oversees INTERPOL in The Hague.[6]

---

[1] *Tasks and Areas of Interest*, AIVD, https://english.aivd.nl/about-aivd/contents/tasks-and-areas-of-interest (last visited June 13, 2016), *archived at* https://perma.cc/63HQ-VC5Z.

[2] *The AIVD's Role in National Security*, AIVD, https://english.aivd.nl/about-aivd/contents/the-aivd%E2%80%99s-role-in-national-security (last visited June 13, 2016), *archived at* https://perma.cc/8H4S-7TFL.

[3] *Id*.

[4] *Id*.

[5] *Netherlands*, INTERPOL, http://www.interpol.int/Member-countries/Europe/Netherlands (last visited June 13, 2016), *archived at* https://perma.cc/LL5U-7M8K.

[6] *Id*.

Other intelligence services are the Military Intelligence and Security Service (Militarie Inlichtengen- en Veiligheidsdients, MIVD),[7] the Fiscal Intelligence and Investigation Service-Financial Control Service,[8] the National Signals Intelligence Organization,[9] the Inspectorate SZW,[10] and the National Coordinator for Security and Counterterrorism (for analysis of threats and coordination of counterterrorism activities).[11]

In mid-2014, the Joint Sigint Cyber Unit (JSCU) began operations as a joint effort launched by the AIVD and MIVD.[12] Under the covenant reached between the two services, the National Sigint Organization, together with other specialized sections of the two services, were merged into the new cooperative arrangement.[13]

---

[7] *Militarie Inlichtengen- en Veiligheidsdients*, MINISTERIE VAN DEFENSIE, http://www.defensie.nl/organisatie/bestuursstaf/inhoud/eenheden/mivd (last visited June 13, 2016), *archived at* https://perma.cc/56LA-XFD7.

[8] *Fiscale Inlichtingen- en Opsporingsdienst - Economische Controledienst (FIOD)*, SOCIALE KAART NEDERLAND, https://landelijk.socialekaartnederland.nl/organisaties/fiscale-inlichtingen-en-opsporingsdienst-economische-controledienst-utrecht (last visited June 13, 2016), *archived at* https://perma.cc/JA26-RXQX.

[9] *Q&A's Nationale Sigint Organisatie*, RIJKSOVERHEID (Mar. 17, 2008), http://www.rijksoverheid.nl/nieuws/2008/03/17/q-a-s-nationale-sigint-organisatie.html, *archived at* https://perma.cc/R8KG-58BV; *see* Ana van Es, *Jagen op terroristen vanuit de polder*, DE VOLKSKRANT (June 23, 2012), http://www.volkskrant.nl/binnenland/jagen-op-terroristen-vanuit-de-polder~a3275554, *archived at* https://perma.cc/P5L9-N69E.

[10] The Inspectorate SZW, instituted on January 1, 2012, combines "the organisations and activities of the former Labour Inspectorate, the Work and Income Inspectorate and the Social and Intelligence Investigation Service of the Ministry of Social Affairs and Employment." *Special Investigation Departments*, RESEARCH AND DOCUMENTATION CENTER, MINISTRY OF SECURITY AND JUSTICE, https://english.wodc.nl/publicaties/bronnengids/politie_opsporing/bijzondere_opsporingsdiensten/ (last visited June 13, 2016), *archived at* https://perma.cc/DU3Z-75FW.

[11] Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV); *see* NATIONAL COORDINATOR FOR SECURITY AND COUNTERTERRORISM, ANNUAL PLAN NCTV 2014, at 3–5 (Jan. 27, 2014) https://english.nctv.nl/Images/nctv-jaarplan2014-27012014-engels-def-internet_tcm92-536300.pdf?cp=92&cs=65023, *archived at* https://perma.cc/9FJE-26A7; ANNUAL PLAN NCTV 2015 (Jan. 20, 2015), https://english.nctv.nl/Images/nctv-jaarplan-2015-en-final-web-lores-los_tcm92-579341.pdf?cp=92&cs=65023, *archived at* https://perma.cc/VHL5-LU57.

[12] *Joint Sigint Cyber Unit, AIVD-MIVD partnership in de praktijk*, NATIONALE VEILIGHEID EN CRISISBEHEERSING (Feb. 2015), https://cyberwar.nl/d/20150226_JSCU-AIVD-MIVD-samenwerking-in-de-praktijk_magazine-nationale-veiligheid-en-crisisbeheersing-2015-nr-1.pdf, *archived at* https://perma.cc/VU7N-ZEHJ. The article has been translated in a personal blog: Matthijs R. Koot, *Dutch Joint Sigint Cyber Unit (JSCU), AIVD-MIVD Partnership in Practice*, MATTHIJS R. KOOT'S NOTEBOOK (Feb. 26, 2015), https://blog.cyberwar.nl/2015/02/joint-sigint-cyber-unit-aivd-mivd-partnership-in-practice, *archived at* https://perma.cc/LS8D-S7TY. For the agreement on the JSCU's establishment, see Kamerbrief over Convenant Joint Sigint Cyber Unit [Parliamentary Paper on the Joint Sigint Cyber Unit Covenant], De Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Defensie, July 3, 2014, https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2014/07/03/kamerbrief-over-convenant-joint-sigint-cyber-unit-jscu/kamerbrief-over-convenant-joint-sigint-cyber-unit-jscu.pdf, *archived at* https://perma.cc/G7B2-MELG.

[13] Didier Bigo et al., *ANNEX 1 – The EU Member States Practices in the Context of the Revelations of NSA Large Scale Operations: 5. The Netherlands*, *in* EU PARLIAMENT, DIRECTORATE-GENERAL FOR INTERNAL POLICIES, NATIONAL PROGRAMMES FOR MASS SURVEILLANCE OF PERSONAL DATA IN EU MEMBER STATES AND THEIR COMPATIBILITY WITH EU LAW 73–74 (2013), http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf, *archived at* https://perma.cc/D8TJ-4WRK. According to this report, "the JSCU is expected to centralize all Signals and Cyber surveillance in the Netherlands and will have a staff of 350. . . . The signals location in Burum and the analysis location in Eibergen, currently operated by the NSO, will stay active." *Id*. at 13. *See also* Kamerbrief over Convenant Joint Sigint Cyber Unit, *supra* note 12, at 1 (announcement preceding the text of the Covenant).

The AIVD shares intelligence analyses with the secret EU Intelligence Analysis Centre (INTCEN), and INTCEN shares its analyses with the AIVD.[14]

II. Legislative Framework

The Intelligence and Security Services Act 2002 governs the activities and powers of the AIVD and also the MIVD.[15] The Act includes provisions on transparency and accountability, measures that "are a direct product of the European Convention on Human Rights."[16]

The AIVD has the authority, among other powers, to observe and follow people, use intelligence agents, and monitor and tap telecommunications. It may use "special powers" (also referred to as "special intelligence resources") only if "strictly necessary" to carry out the duties entrusted to it by law.[17] The special powers include surveillance,[18] using intelligence agents,[19] conducting searches,[20] opening mail "and other consignments" without sender or addressee consent,[21] and monitoring and tapping telecommunications.[22] Special powers cannot be used, however, for security screenings or "safeguarding vital sectors," nor may any act "likely to seriously infringe personal privacy . . . be taken without the express prior permission of the Minister of the

[14] Matthijs R. Koot, *Dutch Govt Response to Parliamentary Questions About EU IntCen*, MATTHIJS R. KOOT'S NOTEBOOK (Jan. 10, 2014), https://blog.cyberwar.nl/2014/01/dutch-govt-response-to-parliamentary-questions-about-eu-intcen, *archived at* https://perma.cc/F7KE-4HQB. This blog post is a translation of responses by Dutch Cabinet members to parliamentary questions about INTCEN.

[15] *The Intelligence and Security Services Act 2002*, AIVD, https://english.aivd.nl/about-aivd/contents/the-intelligence-and-security-services-act-2002 (last visited June 13, 2016), *archived at* https://perma.cc/RV5U-SA5C; Act of 7 February 2002, Providing for Rules Relating to the Intelligence and Security Services and Amendment of Several Acts (Intelligence and Security Services Act 2002), as amended by the Act of 2 November 2006 (Bulletin of Acts, Orders and Decrees 2006, 574), AIVD, https://english.aivd.nl/binaries/aivd-en/documents/publications/2002/03/26/bulletin-of-acts-orders-and-decrees-of-the-kingdom-of-the-netherlands/wiv2002en.pdf, *archived at* https://perma.cc/NH52-WZL3. For the Dutch text of the Act, see Wet op de inlichtingen- en veiligheidsdiensten 2002 (Feb. 7, 2002, mostly in force on May 29, 2002, as last amended effective Jan. 1, 2013), http://wetten.overheid.nl/ BWBR0013409/geldigheidsdatum_14-09-2014, *archived at* https://perma.cc/Z6XW-D6NZ.

[16] *The Intelligence and Security Services Act 2002*, *supra* note 15.

[17] *Powers*, AIVD, https://english.aivd.nl/about-aivd/contents/the-intelligence-and-security-services-act-2002/powers (last visited June 13, 2016), *archived at* https://perma.cc/Y2TP-PEW8.

[18] Intelligence and Security Services Act 2002, art. 20.

[19] *Id*. art. 21.

[20] *Id*. art. 22.

[21] *Id*. art. 23.

[22] *Id*. arts. 24–27. For AIVD's digital intelligence activities, see GENERAL INTELLIGENCE AND SECURITY SERVICE, ANNUAL REPORT 2013, at 18 (Apr. 23, 2014), https://english.aivd.nl/binaries/aivd-en/documents/annual-report/2014/04/23/annual-report-2013/annual-report-aivd-2013.pdf, *archived at* https://perma.cc/Q4KP-JTWC. *See also* GENERAL INTELLIGENCE AND SECURITY SERVICE, ANNUAL REPORT 2015: A RANGE OF THREATS TO THE NETHERLANDS, https://english.aivd.nl/binaries/aivd-en/documents/annual-report/2016/05/26/annual-report-2015-aivd/annual-report-2015-aivd.pdf, *archived at* https://perma.cc/9FGR-2D7E; REVIEW COMMITTEE ON THE INTELLIGENCE AND SECURITY SERVICES, ANNUAL REPORT 2015, http://english.ctivd.nl/binaries/ctivd-eng/documents/annual-reports/2016/06/07/annual-report-2015/ctivd-annual-report-2015.pdf, *archived at* https://perma.cc/M3V3-C7D7.

Interior."[23] The exercise of a special power is generally allowed only if the relevant minister, or the relevant head of a service on the minister's behalf, has given permission for it.[24]

One of the tasks of the AIVD is to conduct investigations regarding other countries on subjects designated by the Prime Minister, in accordance with the relevant ministers.[25] The AIVD is authorized to conduct investigations that involve other countries "regarding matters with military relevance that have been designated by the Prime Minister, Minister of General Affairs in accordance with the relevant Ministers."[26] The AIVD and the MIVD may process the personal data of persons when this is necessary in the context of investigations concerning other countries;[27] tap, receive, record, and monitor conversations, telecommunications, or data transfer by means of an automated network with ministerial permission (with certain exceptions);[28] and receive and record non-cable-bound telecommunications originating from or intended for other countries.[29] Both Services are authorized to notify "the appropriate intelligence and security services of other countries, and the appropriate international security, signals intelligence and intelligence bodies" regarding information processed by or on behalf of the Service.[30]

Both the AIVD and MIVD must submit an annual report before May 1 every year.[31] The Intelligence and Security Services Act 2002 also requires the AIVD to "notify anyone against whom it has used powers which infringe their constitutional right to privacy at home (Article 12) or secrecy of communications (Article 13)."[32] The AIVD must review whether such notification is possible five years after the use of the power in question has terminated, but it will not notify the persons in question if doing so would harm relations with other countries or reveal the sources or methods of the AIVD.[33]

III. Oversight

An independent regulatory commission, comprised of three members appointed by the Crown at the Parliament's recommendation, carries out retrospective monitoring of the AIVD in compliance with the Intelligence and Security Services Act 2002 and also the Security Screening

[23] *Powers*, *supra* note 17.

[24] Intelligence and Security Services Act 2002, art. 19 ¶ 1.

[25] *Id*. art. 6 ¶ 2(d).

[26] *Id*. art. 7 ¶ 2(e).

[27] *Id*. art. 13 ¶¶ 1(c) & 2(c).

[28] *Id*. art. 25 ¶¶ 3 & 8.

[29] *Id.* art. 26 ¶ 1.

[30] *Id*. art. 36 ¶ 1(c).

[31] *Id*. art. 8.

[32] *Notification*, AIVD, https://english.aivd.nl/about-aivd/contents/the-intelligence-and-security-services-act-2002/notification (last visited June 13, 2016), *archived at* https://perma.cc/3P58-9FEB.

[33] *Id*.

Act.[34] "Subject to a legal obligation to confidentiality," the commission "is entitled to inspect any information it wishes."[35] The commission also publishes an annual report.[36]

IV. New Developments

The Dutch government believes that technological developments have overtaken the 2002 Act, and that for the intelligence services to be able to continue to carry out their tasks as well as possible, adjustments in the law are necessary.[37] The desired adjustments would mainly involve the collection of data from telephone, email, and Internet, be it over ether or via cable, to be done only if there is reason to do so, with an independent review beforehand and supervision afterwards.[38] Additional requirements would be imposed to make sure that the privacy of Dutch citizens remains protected as much as possible.[39]

A draft law to address the above concerns is currently under review by the Council of State (an advisory body one of whose major tasks is to advise the government and Parliament on legislation and governance).[40] The current Act has 106 articles; the proposed revision has 151.[41] An explanatory memorandum on the draft law contains appendices that (1) correlate the current Act's provisions and those of the proposed revision; (2) give the detailed structure of the draft law (chapter, section, and paragraph titles); and (3) provide in chart form and overview of the special powers and safeguards found in the draft law.[42] The chart has six categories: the special power concerned; the authority granting permission for it; the duration of the power; the

[34] *Regulatory Commission*, AIVD, https://english.aivd.nl/about-aivd/contents/the-intelligence-and-security-services-act-2002/regulatory-commission, *archived at* https://perma.cc/7QRL-G8EC (last visited June 13, 2016).

[35] *Id*.

[36] *Id*.

[37] *Nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv)* [*New Law on Intelligence and Security Services (Wiv)*], RIJKSOVERHEID, https://www.rijksoverheid.nl/onderwerpen/bevoegdheden-inlichtingendiensten-en-veiligheidsdiensten/inhoud/wet-op-de-inlichtingen-en-veiligheidsdiensten-wiv (last visited June 10, 2016), *archived at* https://perma.cc/WY9S-UVKK.

[38] *Id*.

[39] *Id*.

[40] Wet op de inlichtingen- en veiligheidsdiensten 20.., INTERNETCONSULTATIE [INTERNET CONSULTATION], https://www.internetconsultatie.nl/wiv (consultation period July 2–Sept. 1, 2015), *archived at* https://perma.cc/VXD4-3SYD; *The Council of State*, RAAD VAN STATE, https://www.raadvanstate.nl/the-council-of-state.html (last visited June 13, 2016), *archived at* https://perma.cc/5BYY-PLML.

[41] Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX: wettekst (consultatieversie juni 2015): Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20 [Draft Bill Law on Intelligence and Security 20xx; legislative text (consultation version June 2015): Rules Concerning the Intelligence and Security and Amending Certain Laws (Law on the Intelligence and Security 20..) (of June 2015)], *available at* Internetconsultatie, https://www.internetconsultatie.nl/wiv/document/1715, *archived at* https://perma.cc/FY8W-FGTJ.

[42] Voorstel van Wet op de inlichtingen- en veiligheidsdiensten 20XX; memorie van toelichting (consultatieversie juni 2015): Memorie van Toelichting [Proposed Law on the Intelligence and Security 20XX (Consultation Version June 2015): Explanatory Memorandum], *available at* Internetconsultatie, https://www.internetconsultatie.nl/wiv/document/1721, *archived at* https://perma.cc/R3J6-ACKX.

applicable test (in all cases, necessity, proportionality, and subsidiarity); the data retention/destruction period; and whether the law provides for role separation/job separation/compartmentalization with respect to the special power. In the case of the power of surveillance and monitoring, for example, the power-granting authority is in general the Minister of Security and Justice or the chief of the service, and the duration is a maximum of three months, with a possible three-month extension; the chart indicates the data retention period and the role separation categories do not apply to this power.[43] One of two footnotes attached to the special power category states that to the extent that the exercise of the power takes place against a journalist with the purpose of finding out the journalist's source, the permission of the court in The Hague is required.[44]

The draft legislation is expected to be presented to the Dutch Parliament in the summer of 2016.[45]

[43] *Id*. at 217.

[44] *Id*. at 217 n.203.

[45] *Nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv), supra* note 37.

Sweden

Elin Hofverberg
Foreign Law Research Consultant

SUMMARY Signal surveillance is regulated by Swedish law. Only the National Defense Radio Establishment may carry out surveillance and only on cross-border communications. Information may be requested by the government, the military, and the police. Sweden's surveillance legislation has received widespread criticism, including from the European Parliament, on the grounds that it fails to adequately protect privacy and may violate the European Convention on Human Rights. Specific privacy protection regulations that pertain to surveillance information are in place.

I. Legislative Framework

Collection of intelligence data by signal surveillance is carried out by Försvarets Radioanstalt (FRA) (the National Defense Radio Establishment)[1] and is governed by the Act on Signal Surveillance for Defense Intelligence Activities, commonly referred to as the FRA legislation.[2] Surveillance is also limited by the more general Act on Defense Intelligence Activity.[3]

A. Requirements

Collection of intelligence data by signal surveillance can be requested only by the government, government offices, the Swedish Armed Forces, the Swedish Security Service (Police), and the National Operative Department of the Police.[4] Such collection requires prior authorization from the Defense Intelligence Court[5] and can only be carried out to determine

1. external military threats against the country,
2. conditions for Swedish involvement in peace promotion and humanitarian international missions or threats against the security of Swedish interests during such missions,
3. strategic relationships regarding international terrorism and other significant transborder crimes that can threaten important national interests,

[1] *In English*, FRA, http://www.fra.se/snabblankar/english.10.html (last visited June 8, 2016), *archived at* https://perma.cc/HHG7-MYLA.

[2] LAG OM SIGNALSPANING I FÖRSVARSUNDERRÄTTELSEVERKSAMHET [ACT ON SIGNAL SURVEILLANCE FOR DEFENSE INTELLIGENCE ACTIVITIES] (Svensk författningssamling [SFS] 2008:717), https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2008717-om-signalspaning-i_sfs-2008-717, *archived at* https://perma.cc/K66V-B8DY.

[3] LAG OM FÖRSVARSUNDERRÄTTELSEVERKSAMHET [ACT ON DEFENSE INTELLIGENCE ACTIVITIES] (SFS 2000:130), https://lagen.nu/2000:130, *archived at* https://perma.cc/YJP8-YSQW.

[4] 4 § ACT ON SIGNAL SURVEILLANCE.

[5] *Id*. 4 § 3 para.

4. the development and spread of weapons of mass destruction, military material and products covered in the law (SFS 2000:1064) on control of products with dual uses and technical assistance,
5. serious external threats against the society's infrastructure,
6. conflicts abroad with consequences to international security,
7. foreign intelligence activity against Swedish interests, or
8. the conduct or intentions of foreign government powers that are of considerable importance to Swedish foreign, security or defense policy.[6]

If necessary for security defense intelligence operations, signals in electronic form may also be collected to

1. follow changes in the signal environment abroad, technical developments and signal protection and
2. continuously develop the technology and methods needed to carry out its activity in accordance with this law (2009:967).[7]

The court may grant an application for surveillance only if it conforms to the purposes of the surveillance legislation and the Act on Defense Intelligence Activity, the intelligence need cannot be met in a less invasive manner, and the value of the surveillance clearly outweighs the violations against integrity (human rights).[8] In addition, the application cannot be limited to one specific, physical individual.[9] The Swedish Defense may cooperate with foreign governments in the collection of the abovementioned information.[10]

B. Limitations

The Act on Signal Surveillance limits the scope, duration, and subjects of signal surveillance. The main limitation is that signal surveillance may cover only cross-border communications.[11] Thus, communications that take place solely within the borders of Sweden cannot be legally collected through signal surveillance. However, these limits do not apply to "senders and receivers on foreign state ships, foreign state aircrafts or military vehicles."[12] Domestic surveillance is instead covered by the Swedish law implementing the European Union Data Retention Directive.[13] Moreover, surveillance cannot be targeted against one specific individual alone,[14] and may be approved only for a period of six months at a time.[15]

---

[6] *Id*. 1 § 2 para. (all translations by author).

[7] 1 § 3 para.

[8] *Id*. 5 §.

[9] *Id*.

[10] *Id*. 9 §; 3 § ACT ON DEFENSE INTELLIGENCE ACTIVITIES.

[11] 2a § ACT ON SIGNAL SURVEILLANCE.

[12] *Id*. 2a § 2 para.

[13] The domestic Lagen om elektronisk kommunikation [Act on Electronic Communication] (SFS 2003:389), https://lagen.nu/2003:389, *archived at* https://perma.cc/FX2M-P3HB, is still in force following the EU Court of Justice's invalidation in 2014 of the Data Retention Directive. Case C-293/12, Digital Rights Ireland Ltd. v.

Once collected, stored information must be destroyed by the FRA under certain circumstances—for example, if information on an individual lacks importance to the investigation[16] or the "information was communicated during religious confession or private care of the soul, unless there are exceptional reasons to collect the information."[17]

II. Privacy

Specific privacy legislation deals with the treatment of personal data collected by the FRA.[18] Individuals have the right to inquire whether they are included in the material collected by the FRA.[19] Requests for such information may be made once a year and must be answered within four months.[20] Information may be withheld if secrecy requires it.[21]

Stored data can be shared only with foreign or multinational entities if the information is not protected by secrecy *and* sharing it is required for the FRA to fulfill its international commitments.[22] However, the government has the right to issue regulations that allow secret information to be transferred if considered necessary for the operations of the FRA.[23] The FRA must employ security measures to safeguard personal information.[24]

Only decisions on correction requests and communications of information to third parties may be appealed.[25] Under certain circumstances, such as when information collection constitutes a

---

Minister for Communications, Marine & Natural Res., 2014 E.C.R (2014), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&rid=1, *archived at* https://perma.cc/MS7G-2DP2. For further discussion, see the EU survey.

[14] 4 § 3 para. ACT ON SIGNAL SURVEILLANCE.

[15] *Id*. 5a § 5 item.

[16] *Id*. 7 §.

[17] *Id*.

[18] LAG OM BEHANDLING AV PERSONUPPGIFTER I FÖRSVARSMAKTENS FÖRSVARSUNDERRÄTTELSEVERKSAMHET OCH MILITÄRA SÄKERHETSTJÄNST (SFS 2007:258) [ACT ON THE TREATMENT OF PERSONAL INFORMATION FOR THE INTELLIGENCE ACTIVITIES OF THE SWEDISH DEFENSE AND MILITARY SECURITY SERVICE], https://www.notisum.se/rnp/sls/lag/20070258.htm, *archived at* https://perma.cc/DVL6-Q5XR; LAG OM BEHANDLING AV PERSONUPPGIFTER I FÖRSVARETS RADIOANSTALTS FÖRSVARSUNDERRÄTTELSE- OCH UTVECKLINGSVERKSAMHET [ACT ON THE TREATMENT OF PERSONAL INFORMATION IN THE FRA'S INTELLIGENCE AND DEVELOPMENT ACTIVITIES] (SFS 2007:259), https://www.notisum.se/rnp/sls/lag/20070259.htm, *archived at* https://perma.cc/TR4J-AKWK.

[19] *Id*. 2 ch. 1 § ACT ON THE TREATMENT OF PERSONAL INFORMATION IN THE FRA'S INTELLIGENCE AND DEVELOPMENT ACTIVITIES.

[20] *Id*.

[21] *Id*. 2 ch. 3 §.

[22] *Id*. 1 ch. 17 §.

[23] *Id*.

[24] *Id*. 3 ch. 2 §.

[25] *Id*. 3 ch. 3 §.

violation of personal integrity, the state can be held liable for damages to an individual whose information was illegally obtained.[26]

Sweden has been criticized by the European Parliament for its legislation on signal surveillance, especially as it pertains to privacy protections and its oversight, on the ground that it may violate the European Convention on Human Rights.[27]

III. Oversight Authorities

Sweden has two different oversight authorities for signal intelligence gathering. The oversight authority that oversees the FRA's compliance with the Signal Surveillance Act is Statens inspektion för försvarsunderrättelseverksamheten (Siun),[28] whereas the Swedish Data Inspection Board is responsible for the oversight of privacy issues, specifically how information is stored and shared between agencies.[29] In this capacity the Data Inspection Board has the right to access personal information that has been stored, obtain information about the storage and protection of the collection, and access facilities containing the information.[30] The Board is also responsible for trying to ensure the correction of possible violations.[31] The oversight authority may initiate court proceedings before the district administrative court to have illegally collected information erased.[32] However, the information may not be erased if erasing it is deemed unreasonable.[33]

All government activity is also overseen by the Riksrevisionen (Swedish National Audit Office).[34] In 2015 the Riksrevisionen published a report on FRA surveillance,[35] and has issued a

[26] 2 ch. 5 §.

[27] *EU Scrutinizes Sweden's Surveillance Capacities*, SVERIGES RADIO (Nov. 8, 2013), http://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=5698572, *archived at* https://perma.cc/DNZ8-UPP9; Draft Report on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs, EUR. PARL. DOC. (2013/2188(INI)) (Jan. 8, 2014), http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/moraes_1014703_/moraes_1014703_en.pdf, *archived at* https://perma.cc/EME7-EW2A.

[28] 2 § Förordning med instruktion för Statens inspektion för försvarsunderrättelseverksamheten [Regulation with Instructions for State Inspection of the Defense Intelligence Activity] (SFS 2009:969), http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Forordning-2009969-med-inst_sfs-2009-969, *archived at* https://perma.cc/83WS-VBPG.

[29] Förordning med instruktion för Datainspektionen [Regulation with Instructions for the Data Inspection Board] (SFS 2007:975), http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Forordning-2007975-med-inst_sfs-2007-975, *archived at* https://perma.cc/A5JE-BBJ6.

[30] 5 ch. 2 § ACT ON THE TREATMENT OF PERSONAL INFORMATION IN THE FRA'S INTELLIGENCE AND DEVELOPMENT ACTIVITIES.

[31] *Id*. 5 ch. 3 §.

[32] *Id*. 5 ch. 4 §.

[33] *Id*. 5 ch. 4 § 2 para.

[34] 2 § LAG OM REVISION AV STATLIG VERKSAMHET M.M. [ACT ON AUDITS OF GOVERNMENT ACTIVITIES (SFS 2002:1022), https://www.notisum.se/rnp/sls/lag/20021022.htm, *archived at* https://perma.cc/CMY2-L5EV.

number of recommendations on how FRA surveillance is handed, specifically focusing on the need for Siun to improve its practices for documenting and justifying its activities.[36]

[35] RIKSREVISIONEN, KONTROLL AV FÖRSVARSUNDERRÄTTELSEVERKSAMHETEN [CONTROL OF DEFENSE INTELLIGENCE ACTIVITIES] (RIR 2015:2), http://www.riksrevisionen.se/PageFiles/21131/RiR_2015_02_Anpassad.pdf, *archived at* https://perma.cc/J7LF-UXB2.

[36] *Id*. at 13.

United Kingdom

Clare Feikert-Ahalt
Senior Foreign Law Specialist

SUMMARY Foreign intelligence gathering in the United Kingdom is regulated by the Intelligence Services Act, the Human Rights Act, and the Regulation of Investigatory Powers Act. These Acts provide for a system of warrants to be obtained to conduct surveillance and intercept communications, provided the surveillance is necessary to complete the statutory functions of the relevant agency. Issuing warrants in the UK remains an executive, rather than judicial, act. UK intelligence agencies are subject to parliamentary oversight.

The UK is currently in the process of introducing an Investigatory Powers Bill. This bill, now before the House of Lords, would substantially repeal and re-enact the majority of the legal framework governing the interception of communications. The aim of the bill is to provide a clearer framework of powers and oversight. The bill would also require judicial approval of warrants issued by the Secretary of State and provide for the enhanced ability to intercept Internet communications records, which contain more information than communications data. It would also allow for the interception and retention of data in bulk. As with all previous bills that address the interception of communications, there has been significant criticism that the provisions are still not clear enough and are too wide-ranging. The government claims that the bill would essentially re-enact existing legislation and that the limited expansion of powers is necessary to fill gaps in the ability of law enforcement and the intelligence services to keep the country safe.

I. Introduction

The UK has three intelligence and security agencies, which are commonly referred to collectively as the Agencies or the Intelligence Services. These Agencies consist of the Secret Intelligence Service (SIS), also known as MI6 ("MI" standing for Military Intelligence), the UK's overseas intelligence agency; the Government Communications Headquarters (GCHQ), the UK's signals intelligence gathering agency; and the Security Service, also known as MI5, the UK's domestic intelligence agency. The Security Service has statutory responsibility to protect the national security of the UK from international threats, including those from terrorism. It is supported in this role by the SIS and GCHQ, who provide intelligence gathered from overseas.[1]

While these are the primary agencies in charge of collecting, gathering, and analyzing intelligence information, they are not the only parts of the intelligence machinery in the UK. Additional intelligence is compiled by the Cabinet Office, Defence Intelligence (part of the Ministry of Defence), and the Joint Terrorism Analysis Centre (JTAC).[2] The National Crime

[1] Intelligence and Security Committee, Report into the London Terrorist Attacks on 7 July 2005, 2006, Cm. 6785.

[2] NATIONAL INTELLIGENCE MACHINERY, 2010, at 1, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61808/nim-november2010.pdf, *archived at* https://perma.cc/K3PH-26B7.

Agency addresses organized crime and economic crime that occurs within the UK's borders.[3] All of these agencies must act within the bounds of the law and their operations "must relate to national security, the prevention or detection of serious crime, or the UK's economic well-being."[4]

II. Legislative Framework

The work of the SIS and GCHQ is undertaken in accordance with the legislative framework of the Human Rights Act,[5] the Regulation of Investigatory Powers Act (RIPA),[6] and the Intelligence Services Act 1994 (the ISA),[7] which placed the SIS and GCHQ on a statutory footing and under the responsibility of the Foreign Secretary.

The ISA defines the function of the SIS as follows:

> (a) to obtain and provide information relating to the actions or intentions of persons outside the British Islands; and
> (b) to perform other tasks relating to the actions or intentions of such persons.[8]

The GCHQ's role is defined as follows:

> (a) to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material; and
>
> (b) to provide advice and assistance about—(i) languages, including terminology used for technical matters, and (ii) cryptography and other matters relating to the protection of information and other material, to the armed forces of the Crown, to Her Majesty's Government in the United Kingdom or to a Northern Ireland Department or to any other organisation which is determined for the purposes of this section in such manner as may be specified by the Prime Minister.[9]

These functions may only be exercised in the interests of national security with regard to the defense and foreign policies of the UK, in the interests of the economic well-being of the UK, and in support of the prevention or detection of serious crime.[10]

---

[3] *About the NCA*, NATIONAL CRIME AGENCY, http://www.nationalcrimeagency.gov.uk (last visited June 14, 2016), *archived at* https://perma.cc/VF2R-XQUF.

[4] NATIONAL INTELLIGENCE MACHINERY, *supra* note 2, at 2.

[5] Human Rights Act 1998, c. 42, http://www.legislation.gov.uk/ukpga/1998/42, *archived at* https://perma.cc/Y75U-VDHL.

[6] Regulation of Investigatory Powers Act 2000, c. 23, http://www.legislation.gov.uk/ukpga/ 2000/23/contents, *archived at* https://perma.cc/FKT4-V8NF.

[7] Intelligence Services Act 1994, c. 13, http://www.legislation.gov.uk/ukpga/1994/13/contents, *archived at* https://perma.cc/Y3HW-Z98A.

[8] *Id*. § 1(1).

[9] *Id*. § 3(1).

[10] *Id*. § 1(2).

The ISA provides for a system of warrants that authorize entry on and interference with property or with wireless telegraphy upon application from any of the three Intelligence Services.[11] Due to the important role the Intelligence Services play in safeguarding the UK's national security, the ISA's requirements for an authorization are much broader than those for the Acts that cover domestic surveillance.

Each warrant must be approved by the Secretary of State.[12] The Secretary of State must believe that the conduct is proportionate and necessary to assist the Security Service, SIS, or GCHQ in conducting any of their functions under their respective Acts and that the information sought cannot be obtained by other means.[13] Warrants provided to the SIS and GCHQ for the purposes of preventing or detecting crime may not relate to the British Islands. The Intelligence Services Act was amended by the Prevention of Terrorism Act 2005, which provides the Intelligence Services authority to obtain a warrant to conduct activities in the UK as well as overseas. The Security Service also can obtain a warrant to interfere with property or wireless telegraphy if it is acting on behalf of the SIS or GCHQ and the action proposed is to be "undertaken otherwise than in support of the prevention of detection of serious crime."[14]

III. Interception of Communications

The use of covert surveillance, use of covert human intelligence sources,[15] and interception of both communications and communications data in England and Wales is allowed, provided the relevant laws regulating this procedure are adhered to.[16]

There is no single legislative regime that applies to the interception of communications; instead the laws and procedures vary according to the body that is seeking the interception. The main piece of legislation in this area is the Regulation of Investigatory Powers Act 2000 (RIPA).[17]

[11] *Id*. § 5.

[12] The Secretary of State may also issue warrants to enable the SIS or GCHQ to conduct actions outside the UK. These are known as section 7 warrants, and their purpose is to help protect officers and agents from these agencies from prosecution in the UK. RT. HON. SIR MARK WALLER, INTELLIGENCE SERVICES COMMISSION, REPORT OF THE INTELLIGENCE SERVICES COMMISSIONER FOR 2013, H.C. 302, at 57, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/324152/Intelligence_Services_Commissioner_Accessible__2_.pdf, *archived at* https://perma.cc/4S6M-LBNW.

[13] Intelligence Services Act 1994, c. 13, § 5, http://www.legislation.gov.uk/ukpga/1994/13, *archived at* https://perma.cc/G7VW-XVYZ.

[14] *Id*. § 5(4), (5).

[15] Directed surveillance may be authorized by a designated person within each of the intelligence services provided that it is necessary to fulfill the agency's statutory functions, is undertaken for the purpose of a specific investigation, is proportionate, and cannot be achieved through other means. Regulation of Investigatory Powers Act 2000, c. 23, § 28.

[16] The Regulation of Investigatory Powers Act provides that unlawfully intercepting communications is an offense punishable by up to two years' imprisonment and/or a fine. *Id*. § 1.

[17] *Id*.

RIPA serves to augment the ISA, providing for distinct authorization processes for warrants that apply to the interception of communications[18] and the interception of communications data.[19]

Before the Secretary of State can authorize a warrant to intercept communications, he must believe that the conduct requested by the warrant cannot be obtained by other means, is proportionate and necessary in what it is seeking to achieve, and has as its purpose one of the following: protecting the interests of national security, preventing or detecting serious crime,[20] safeguarding the economic well-being of the UK from the acts or intentions of individuals outside the British Isles, or giving effect to an international mutual assistance agreement whose purpose is equivalent to that of preventing or detecting serious crime.[21] Before signing the warrant, the Secretary of State must also consider whether the warrant is operationally required and if its issuance is proportionate and necessary.[22]

RIPA provides for the lawful acquisition and disclosure of communications data in specified circumstances. Communications data does not include the content of a communication but the information that relates to the use of a communications service; thus the requirements to obtain an authorization are less stringent and the list of individuals who can request an authorization is less restrictive. An authorization to obtain communications data can only be obtained if necessary in the interests of national security or the economic well-being of the UK; for the purposes of preventing or detecting crime or preventing disorder; in the interests of public safety; for assessing or collecting a tax, duty, levy or other imposition; or for protecting public health or, in an emergency, preventing death, injury, or damage to an individual's physical or mental health, or mitigating such damage.[23]

The range of officials who can authorize the interception of communications data is much broader than in other areas of surveillance, and such authorization can be granted by a senior official in the relevant public authority.[24]

[18] "Communication" is defined broadly in section 81 of the Regulation of Investigatory Powers Act, *id*.

[19] Communications data includes subscriber data, use data, and traffic data. SECRETARY OF STATE FOR THE HOME DEPARTMENT, DRAFT COMMUNICATIONS DATA BILL, 2012, Cm. 8359, ¶ 10, http://www.official-documents.gov.uk/document/cm83/8359/8359.pdf, *archived at* https://perma.cc/R5PZ-HF8E.

[20] Detecting crime is interpreted in section 81 of the Regulation of Investigatory Powers Act as "(a) establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed; and (b) the apprehension of the person by whom any crime was committed."

[21] *Id*. § 5.

[22] *Id*.

[23] *Id*. § 22(2).

[24] *Id*. § 22; 2 CURRENT LAW STATUTES 2000 (Christine Beesley et al. eds., 2000).

IV. Oversight

The Intelligence Agencies are also subject to parliamentary oversight by the Intelligence and Security Committee, which operates within the "ring of secrecy" to examine the expenditure, administration, and policy of all the Intelligence Agencies.[25] RIPA further requires that the Prime Minister appoint an Intelligence Services Commissioner to review how the Secretary of State issues warrants for both surveillance and interference with property by the Intelligence Services, as well as how the Secretary of State exercises and performs the powers and duties granted by RIPA in relation to the Intelligence Services, although the power to review warrants by this Commissioner is retrospective.[26]

V. Investigatory Powers Bill 2015-16

The government stated in 2015[27] that it would introduce a new Investigatory Powers Bill to regulate the interception of communications data.[28] The bill was published in draft form in November 2015,[29] with the government emphasizing that it did not create a series of new powers, but merely served to repeal and re-enact in a clearer manner existing powers already provided for in legislation. The draft bill was reviewed by three parliamentary committees,[30] which criticized the existing framework of investigatory powers,[31] noting that the existing

[25] The role of the ISC has recently been amended and clarified by the Justice and Security Act 2013, c. 18, http://www.legislation.gov.uk/ukpga/2013/18/contents/enacted, *archived at* https://perma.cc/LU5A-GFLM.

[26] Regulation of Investigatory Powers Act 2000, c. 23, § 59(1)–(2).

[27] PRIME MINISTER'S OFFICE, THE QUEEN'S SPEECH 6 (May 27, 2015), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/430149/QS_lobby_pack_FINAL_NEW_2.pdf, *archived at* https://perma.cc/N7N8-LTHQ.

[28] DAVID CAMERON, THE REPORT OF THE INVESTIGATORY POWERS REVIEW: WRITTEN STATEMENT, June 10, 2015, HCWS27, http://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2015-06-11/HCWS27, *archived at* https://perma.cc/U5CS-QZTJ.

[29] DRAFT INVESTIGATORY POWERS BILL, Cm. 9152, 2015-16, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf, *archived at* https://perma.cc/8YV2-RSYW.

[30] David Anderson, QC, *A Question of Trust*, June 2015, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf, *archived at* https://perma.cc/SEQ5-7TSW. This report recommended that the Regulation of Investigatory Powers Act be replaced with new legislation that bulk collection of intercepted materials should be permitted under strict safeguards; the Home Secretary's role in authorizing the interception of communications should be restricted and replaced with judicial oversight; the definition of communications data should be updated; and a new position, the independent surveillance and intelligence commissioner, should be created and should replace the three current commissioners. INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT, REPORT ON THE DRAFT INVESTIGATORY POWERS BILL, HC 795, 2015-16, http://isc.independent.gov.uk/files/20160209_ISC_Rpt_IPBill(web).pdf, *archived at* https://perma.cc/CSK2-AS7M. This report criticized the current legal framework as being developed in a piecemeal way and that it was unnecessarily complicated, resulting in a lack of transparency. RUSI, *A Democratic Licence to Operate: Report of the Independent Surveillance Review*, July 2015, https://rusi.org/publication/whitehall-reports/democratic-licence-operate-report-independent-surveillance-review, *archived at* https://perma.cc/BC47-ZAZG. This report claimed that the existing law was too complex and there were inadequacies in oversight.

[31] DRAFT INVESTIGATORY POWERS BILL REPORT, HL 93, HC 651, 2015-16, http://www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/93.pdf, *archived at* https://perma.cc/W785-8TA2; INTELLIGENCE

legislation had developed in a patchwork fashion and was in need of reform.[32] The disclosures of Edward Snowden also highlighted the need for a new, clearer legislative framework to govern the interceptions of communications. Snowden's disclosures caused significant concern among UK citizens that the government was collecting data about them *en masse*, and led technology companies to improve privacy protections and strengthen the encryption they offer their customers, the results of which have been to place many communications outside the reach of the intelligence agencies and courts.[33]

The bill was introduced in the House of Commons on March 1, 2016.[34] The bill has passed through the House of Commons and is currently awaiting its second reading in the House of Lords.[35] Prime Minister David Cameron has stated there is a pressing need for the bill to be enacted before the sunset provision of the Data Retention and Investigatory Powers Act 2014 takes effect on December 31, 2016,[36] which would leave law enforcement and the intelligence services without lawful authority to intercept certain communications absent passage of a replacement measure. The bill aims to modernize the laws on communications data[37] and bring together all investigatory powers available to law enforcement and the intelligence services.

A. Provisions in the Bill

The Investigatory Powers Bill is substantive, containing 243 sections and ten schedules in 268 pages. If enacted, it will repeal and replace almost the entire system that regulates the

---

AND SECURITY COMMITTEE OF PARLIAMENT, *supra* note 30; HOUSE OF COMMONS SCIENCE AND TECHNOLOGY COMMISSION, INVESTIGATORY POWERS BILL: TECHNOLOGY ISSUES, THIRD REPORT OF SESSION 2015-2016, HC 573, 2015-16, http://www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/573/573.pdf, *archived at* https://perma.cc/5PYM-FQF2. The government responded to these reports in the following report: INVESTIGATORY POWERS BILL: GOVERNMENT RESPONSE TO PRE-LEGISLATIVE SCRUTINY, Cm 9219, 2015-16, https:/ /www.gov.uk/government/uploads/system/uploads/attachment_data/file/504174/54575_Cm_9219_WEB.PDF, *archived at* https://perma.cc/N35G-DZXG.

[32] *Investigatory Powers Bill*, HOUSE OF COMMONS LIBRARY, Mar. 11, 2016, http://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7518, *archived at* https://perma.cc/96TD-5QPH.

[33] INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT, PRIVACY AND SECURITY: A MODERN AND TRANSPARENT LEGAL FRAMEWORK, 2014–15, HC 1075, ¶ 4, http://isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf, *archived at* https://perma.cc/GNT4-G4XS.

[34] *Investigatory Powers Bill 2015-16 to 2016-17*, PARLIAMENT.UK, http://services.parliament.uk/bills/2015-16/investigatorypowers.html, *archived at* https://perma.cc/SXB3-L3ED. The provisions of the Bill as introduced to the House of Commons are available at: *Investigatory Powers Bill (HC Bill 2)*, PARLIAMENT.UK, http://www.publications.parliament.uk/pa/bills/cbill/2016-2017/0002/17002.pdf, *archived at* https://perma.cc/L5FA-2NSJ. The current version of the bill is available at: Investigatory Powers Bill 2015-16, HL Bill 40, http://www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040.pdf, *archived at* https://perma.cc/8ZVS-V8CE. As the bill is controversial, there are many amendments, and the clauses and numbering are frequently changed.

[35] *Investigatory Powers Bill 2015-16 to 2016-17*, PARLIAMENT.UK, http://services.parliament.uk/bills/2016-17/investigatorypowers.html (last visited June 13, 2016), *archived at* https://perma.cc/NTY2-TPAB.

[36] *Id.*; Data Retention and Investigatory Powers Act 2014, c. 27 § 8(3), http://www.legislation.gov.uk/ukpga/2014/27/ contents/enacted, *archived at* https://perma.cc/Y2ZC-4NNN. This Act was enacted as emergency legislation and passed through Parliament in four days with cross-party support.

[37] *Id.* at 8.

interception of communications.[38] The main parts of the bill address the interception of communications, the retention and acquisition of communications data, equipment interference, the retention and examination of bulk personal datasets, and the decryption of communications. These are areas where the government claims the gap in capabilities is putting lives at risk, and addressing these areas would enable law enforcement to effectively target terrorist communications.[39] The bill provides for these powers to be used on both a targeted basis and, in certain instances, for the collection, retention, and examination of bulk datasets.[40] The government claims that the only new capability provided for in the bill is the ability to require the retention of Internet connection records, which the Home Secretary has compared to itemized phone bills as it shows the websites that an individual has visited.[41]

1. Interception of Communications

Chapter 1 of the bill provides the process for the lawful interception of communications. There are three different types of interception and examination warrants that would be authorized under this part of the bill:

- Targeted interception warrants. This authorizes the interception of communications and the acquisition of associated communications data that relates to a particular organization, person, premises, or group of connected to subjects that are part of a single investigation.[42]
- Targeted examination warrants. This authorizes the examination of intercepted materials obtained by a bulk interception warrant.
- Mutual Assistance warrants. This allows requests for assistance with overseas interception.[43]

Interference with communications in certain instances and locations is lawful without a warrant and the bill clarifies these circumstances. These instances include when there is consent to the interception; if the interception occurs in a prison, psychiatric hospital, or immigration detention facility; or if the interception is for regulatory enforcement or business purposes.[44]

2. Warrant Authorization for the Interception of Communications

The process to obtain warrants varies according to the type of information for which interception is sought. Given that intercepting communications covers the content of those communication, the criteria and authorities permitted to intercept communications is more stringent than that required to intercept communications data.

---

[38] Investigatory Powers Bill 2015-16, HL Bill 40, http://www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040.pdf, *archived at* https://perma.cc/8ZVS-V8CE. Repeals are provided for throughout the bill.

[39] PRIME MINISTER'S OFFICE, *supra* note 27, at 6.

[40] HOUSE OF COMMONS LIBRARY, *supra* note 32.

[41] *Id*.

[42] Investigatory Powers Bill 2015-16, HL Bill 40, clause 15.

[43] Bill Part I; HOUSE OF COMMONS LIBRARY, *supra* note 32, at 19.

[44] Investigatory Powers Bill 2015-16, HL Bill 40, Chapter 2.

Under the bill, the heads of the intelligence services, National Crime Agency, the Police, HM Revenue and Customs, and Chief of Defence Intelligence, and a competent authority from another jurisdiction as part of a mutual assistance agreement, would be known as "intercepting authorities" who may apply for a warrant to intercept communications. The Secretary of State would be able to issue a warrant to intercept communications if he or she believes it is necessary on the grounds of national security, for the prevention or detection of serious crime, to safeguard the economic well-being of the UK, to preserve national security, or to give effect to an international mutual assistance agreement. The warrant must be proportionate to the goal that it seeks to achieve.[45]

In a substantial change from the current system used to authorize warrants, the decision of the Secretary of State would then need to be approved by a Judicial Commissioner. When reviewing the decision, the Judicial Commissioner would be required to consider whether the Secretary of State met the test of necessity and proportionality when granting the warrant, using the same criteria as a court would during judicial review,[46] meaning that the lawfulness of the decision would be determined according to the process the Secretary of State used to make it.[47] Provided the decision process was reasonable and rational, or in cases where human rights and EU law were involved, the decision was also proportionate to the objective it sought to achieve, the warrant would stand.[48] The Judicial Commissioner could refuse to approve the warrant if he or she feels that the tests have not been met, and must set out the grounds for the decision in writing. The agency that requested the warrant could then attempt to address the concerns and resubmit the request. If the Judicial Commissioner refused to approve the warrant again, the application could be sent to the Information Commissioner for reconsideration. There would be no further course for appeal if the Information Commissioner refused to approve the warrant.[49] In urgent cases, approval of the Judicial Commissioner would not be necessary, but would need to be obtained within three days. If the Judicial Commissioner did not approve the warrant, it would cease to have any effect and the Judicial Commissioner would have discretion to determine what happened to any intelligence or material gathered during the period the warrant was lawfully in effect.

Critics have expressed concern that the judicial oversight provided is too narrow as it looks only at whether the process and reasonableness of the home secretary's decision rather than the merit and substance of the warrant.[50]

[45] *Id*. clauses 15-25.

[46] HOUSE OF COMMONS LIBRARY, *supra* note 32, ¶ 3.4.

[47] *Id*.

[48] *Id*.

[49] Investigatory Powers Bill 2015-16, HL Bill 40, clauses 23-25.

[50] HOUSE OF COMMONS LIBRARY, *supra* note 32, at 23.

3. Warrant Authorization for the Interception of Communications Data

The number of authorities that may request a warrant for the interception of communications data is wider and includes the intelligence services, law enforcement agencies, government departments, regulatory bodies, and the National Health Service. A designated person from these agencies may grant a warrant if they are satisfied that it is necessary and proportionate, and related to one of the ten following grounds:

- In the interests of national security
- To prevent or detect crime, or prevent disorder
- In the interests of the economic well-being of the UK if these are also relevant to the national security of the UK
- In the interests of public safety
- To protect public health
- To assess or collect any tax, duty, levy, or charge payable to a government department
- To prevent death, injury, or damage to a person's mental or physical health, or mitigate any injury or damage
- To assist into any investigation into the miscarriage of justice
- To assist in the identification of any person who has died or who is unable to identify themselves due to a physical or mental condition
- To exercise functions relating to the regulation of financial services and markets or financial stability[51]

Except in urgent cases, prior to granting the authorization, the designated senior officer would have to consult with "an officer in a relevant public authority trained to facilitate lawful acquisition of communications data and effective cooperation between public authorities and CSPs."[52]

4. Interception of Internet Connection Records

The interception of Internet connection records is provided for in clause 59, which states that these records may only be obtained to identify the sender of an online communication, the communication service a person has used, where the person has accessed illegal content, which Internet service is being used, and when and how it is being used.[53] Any authorization obtained

[51] Investigatory Powers Bill 2015-16, HL Bill 40, clauses 58(7). This substantively re-enacts the provisions contained in Chapter 2, Part 1 of RIPA. Clauses 66 and 69 list the public authorities that may obtain communications data under these provisions; the minimum office or rank of the designated senior officer, the types of communications data that may be obtained and the purposes that they may be obtained.

[52] HOUSE OF COMMONS LIBRARY, *supra* note 32, at 3. This officer would be known as the single point of contact. Investigatory Powers Bill 2015-16, HL Bill 40, clause 72.

[53] Investigatory Powers Bill 2015-16, HL Bill 40, clause 59.

under this provision is valid for one month, although it may be renewed or cancelled.[54] The bill creates a duty on communications service providers to comply, as far as reasonably practicable, with any request for communications data.[55] Information that may be obtained under this section includes communications data for the purposes of identifying a journalist's source of information. The approval of the Judicial Commissioner is required in cases where a public authority wishes to obtain this information.[56]

In cases where a complex request for data is made, clauses 63–65 would provide the Secretary of State with the ability to establish a "request filter" system, where any material that is not directly relevant to an investigation would be filtered and deleted before the data is supplied. This filter would be overseen by the Investigatory Powers Commissioner, who would be required to submit an annual report on the operation of this system.[57]

These provisions are among the most controversial of the bill. Internet connection records were initially described by the Home Secretary as being the equivalent of an itemized phone bill.[58] The definition of "Internet connection records" has been criticized as being vague.[59] Individuals in the technology sector have expressed concern that the term does not exist within the industry and the information required to be collected is not within a recognized data type.[60] The lack of clarity regarding the meaning of Internet connection records has also led many within the technology sector to express concern that the cost of compliance with the bill, and the impact on businesses and consumers, cannot be accurately assessed.[61]

5. Interception of Communications of Members of Parliament

There has been a convention, known as the Wilson Doctrine, that communications of Members of Parliament should not be intercepted by the Intelligence Services or police.[62] A recent case determined that this doctrine did not have any legal effect, however.[63] The bill places the ability

[54] *Id*. clause 61.

[55] *Id*. clause 62.

[56] *Id*. clause 61.

[57] *Id.* clauses 63–65.

[58] *Written Evidence from the Home Office (IPB0146), Volume of Written Evidence*, at 522, https://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf, *archived at* https://perma.cc/7JZL-YV9C.

[59] Scott Carey, *Snooper's Charter: What You Need to Know About the Investigatory Powers Bill*, COMPUTERWORLDUK (June 8, 2016), http://www.computerworlduk.com/security/draft-inestigatory-powers-bill-what-you-need-know-3629116, *archived at* https://perma.cc/94F6-JVEN.

[60] DRAFT INVESTIGATORY POWERS BILL REPORT, *supra* note 31, ¶¶ 109–126.

[61] HOUSE OF COMMONS LIBRARY, *supra* note 32, at 36.

[62] 736 HANSARD (4th ser.) 1966 634–41, http://hansard.millbanksystems.com/commons/1966/nov/17/telephone-tapping, *archived at* https://perma.cc/UG95-Y56A. *See also* House of Commons Library, *The Wilson Doctrine*, Briefing Paper No. 4258, Feb. 9, 2016, http://researchbriefings.files.parliament.uk/documents/SN04258/SN04258.pdf, *archived at* https://perma.cc/8Q8C-M2R5.

[63] Caroline Lucas et al. v. Security Service et al., [2015] UKIPTrib 14 79-CH, http://www.ipt-uk.com/docs/Caroline_Lucas_JUDGMENT.pdf, *archived at* https://perma.cc/X3JP-KQHN.

of law enforcement to conduct equipment interference and intercept the communications of Members of Parliament on a statutory basis. Prior to approving any warrant to undertake these activities, the Secretary of State must consult with the Prime Minister.[64]

6. Retention and Use of Intercepted Material

Clause 83 provides the Secretary of State with the ability to issue a retention notice to communications service providers that would require them to retain communications data for up to twelve months.[65] The Secretary of State may issue one of these notices if he or she considers that one of the grounds for issuing an authorization to intercept communications data is met and that the retention is necessary and proportionate. The retention notice can apply to more than one operator and all data or to a specified type of data for up to twelve months. Prior to issuing a retention notice, the Secretary of State must take into account a number of factors, including the benefits of any information obtained from the notice; the potential number of users that the notice relates to; the technical feasibility of complying with the notice; and the effect on the communications service provider. Prior to giving the notice, the Secretary of State should take reasonable steps to consult with any communications service provider to whom the notice relates.[66]

There is a review process for data retention notices by the Secretary of State. In certain circumstances, the specifics of which will be provided for at a later date in regulations, the operator that receives a retention notice may refer the notice back for review by the Secretary of State, who must undertake the review in consultation with the Technical Advisory Board and the Investigatory Powers Commissioner. Until the review is complete, there is no obligation to comply with the requirements in the notice.[67] During the review, the technical requirements and financial consequences of compliance with the notice will be considered, as well as whether the notice is proportionate. The Secretary of State may then affirm, vary, or revoke the retention notice. The Communication Service Provider must have steps in place to ensure that data retained in compliance with the notice is securely stored, protected against unlawful disclosure, and destroyed when it is no longer authorized.[68]

7. Equipment Interference

Equipment interference (also known as computer network exploitation) involves accessing individuals' devices and computers to obtain data, which includes geolocation, text messages, and emails, and also allows law enforcement agencies to access encrypted communications.[69] The bill provides for the process to authorize equipment interference to obtain communications or private information that would otherwise be an offence under the Computer Misuse Act

[64] HOUSE OF COMMONS LIBRARY, *supra* note 32, at 18; Investigatory Powers Bill 2015-16, HL Bill 40, clause 26.

[65] Investigatory Powers Bill 2015-16, HL Bill 40, clause 83.

[66] *Id*. clause 84.

[67] *Id*. clause 85.

[68] *Id*. clauses 86–87.

[69] HOUSE OF COMMONS LIBRARY, *supra* note 32, at 42.

1990.[70] The bill provides for targeted equipment interference, which would authorize the interference with equipment to obtain communications, private information or equipment data, and allow the recipient to get, monitor, examine, and disclose any material obtained as a result of the warrant. Targeted examination authorizes the person to examine material obtained under a bulk equipment interference warrant. As with warrants to intercept communications, warrants for equipment interference may apply to a specific person, group of people, organization, multiple organizations, or a specific location or locations where the equipment is located.[71] The warrant may also be targeted at equipment where there is a link between different people, locations, or organizations if it is necessary for the purposes of a single investigation.

The Secretary of State may issue a warrant to authorize equipment interference upon application by the heads of the intelligence services where it is necessary on the grounds of national security, the prevention or detection of serious crime, or the interests of the economic well-being of the UK, and proportionate to the objective that it is seeking to achieve.[72]

Law enforcement may also obtain a warrant for equipment interference if it is necessary and proportionate for the purposes of preventing and detecting serious crime, or other purposes if necessary to prevent death or serious harm to a person's physical or mental health.[73] The warrant must be personally signed by the Secretary of State and approved by a judicial commissioner applying the principles of judicial review.[74]

Warrants issued under these provisions continue in force for up to six months, but may be renewed, modified or canceled.[75]

Items covered by legal privilege may be the subject of a targeted equipment interference or examination warrant and in these cases, the warrant would need to specify that it is the intention to obtain this information, and exceptional and compelling circumstances must exist to justify the warrant.[76]

As with warrants to intercept communications, communications service providers have a duty to assist with the implementation of any equipment interference warrant[77] and must take all steps necessary to give effect to the warrant. The bill contains provisions that aim to not unreasonably burden providers when complying with its provisions. Communications service providers are not required to take any steps that are not reasonably practicable for them to take;[78] however; the

[70] Computer Misuse Act 1990, c. 18, http://www.legislation.gov.uk/ukpga/1990/18, *archived at* https://perma.cc/G963-P2QN.

[71] HOUSE OF COMMONS LIBRARY, *supra* note 32, at 44.

[72] *Id*.

[73] Investigatory Powers Bill, 2015-16, HL Bill 40, clause 96.

[74] *Id*. clauses 97–99.

[75] *Id*. clause 108.

[76] *Id*. clause 100.

[77] *Id*. clause 120.

[78] *Id*.

Secretary of State may enforce on any person in the UK the duty to comply with a warrant. This may be done through civil proceedings for an injunction or specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or through proceedings to obtain "any other appropriate relief."[79]

Safeguards must be in place to protect any data acquired by the warrant, and equivalent safeguards to those that exist in the UK must be in place before any material is shared with an agency located overseas.[80] The offense of unauthorized disclosure applies to the details or existence of a warrant, and to any material obtained under it.[81]

There have been numerous objections to the proposed equipment interference provisions in the bill, with critics claiming that the bill does not acknowledge the "dangers inherent with equipment interference."[82]

8. Warrants for Bulk Data

The bill provides for a number of warrants that would authorize the acquisition of data in the form of bulk interception warrants, bulk communications warrants, bulk equipment interference warrants, and bulk personal dataset warrants.[83]

Bulk communication warrants would enable the collection of bulk communications of individuals outside the British Islands, which includes the UK, Guernsey, Jersey, and the Isle of Man, followed by the selection of specific communications to be reviewed. Warrants would only be issued where the main purpose it to obtain overseas communications or other data on specific grounds, one of which must be national security. The heads of the intelligence services, or someone acting on their behalf, would be responsible for applying for a warrant, which must be personally signed by the Secretary of State and approved by a Judicial Commissioner.

The provisions that apply to bulk interception warrants also apply to bulk acquisition warrants. The main difference is that these warrants would be available for domestic communications, and communications service providers could be required to disclose specific communications data, or they may be required to obtain and then disclose data if they do not have it. A targeted examination warrant is required to examine material of any person within the British Islands.[84]

Bulk equipment interference warrants would allow the collection of data relating to a number of devices and enable the intelligence services to collect data from a number of devices without

[79] *Id*.

[80] *Id*. clause 122.

[81] *Id*. clause 123.

[82] *Briefing and Response to New Investigatory Powers Bill*, TECHUK.ORG (Mar. 2, 2016), https://www.techuk.org/insights/news/item/7847-techuk-issues-detailed-response-and-briefing-on-new-ip-bill, *archived at* https://perma.cc/R9L4-S5QV.

[83] Investigatory Powers Bill 2015-16, HL Bill 40, part 6.

[84] HOUSE OF COMMONS LIBRARY, *supra* note 32, at 52.

targeting specific people, equipment, or activities. These warrants aim to obtain overseas-related communications, private information, or equipment data. As with bulk interception, a targeted examination warrant is required to examine material of any person within the British Islands.[85]

Warrants may also be obtained for bulk personal datasets. This would enable the intelligence services to apply for two types of warrants to intercept datasets in bulk. A class warrant would enable the intelligence services to retain and examine bulk datasets about a large class of people that must be described in the warrant, and the majority of people within this class are not of interest to the agencies—for example, a list of people who are in possession of a passport.[86] The intelligence services would only be able to retain or examine a bulk personal dataset with a warrant under these provisions if the material does not fall under another warrant provided for in the bill.

A "specific warrant" is also provided for in the bill, which would allow the intelligence services to retain and examine bulk personal data that is described in the warrant.[87] These warrants would be necessary if the dataset does not fall in a class of information that could be covered by a class warrant, the dataset contains novel or new information, or in cases where the "dataset may raise issues of sensitivity such that it would be appropriate for the Secretary of State to issue a specific warrant."[88] In cases of both types of warrants, no data that is held in the bulk dataset may be examined unless it is necessary for the operational purposes specified in the warrant.[89] Only trained staff may access the datasets, and any search "must be justified on the basis of necessity and proportionality and for one of the authorised operational purposes."[90]

The Secretary of State must authorize warrants for bulk personal datasets and specific warrants and believe that it is necessary on the grounds of national security, serious crime, or economic well-being of the UK where relevant to national security. The warrant must be proportionate to the objective that it seeks to achieve and satisfactory arrangements must be in place to handle data. The warrant must then be approved by a Judicial Commissioner.[91]

Warrants continue in force for up to six months, and may be renewed, modified or cancelled. In cases where the warrant expires or is cancelled, in order to retain and examine the dataset a new warrant must be applied for within three months.[92] UK datasets from the UK must be examined

[85] *Id.*

[86] *Id.* at 58.

[87] *Id.*

[88] *Id.*

[89] *Investigatory Powers Bill*, GOV.UK, at 2, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/505505/Bulk_Personal_Dataset_factsheet.pdf (last visited June 14, 2016), *archived at* https://perma.cc/A9N8-2ZTW.

[90] *Id.*

[91] HOUSE OF COMMONS LIBRARY, *supra* note 32, at 58.

[92] Investigatory Powers Bill, 2015-16, HL Bill 40, clause 189.

within three months, and datasets originating from overseas must be examined with six months.[93]

Provisions that allow for bulk interception and interference have been among the most controversial in the bill, with many critics asserting that it provides intelligence agencies with the ability to undertake mass surveillance.[94] Critics argue that the routine collection of bulk information gives rise to privacy concerns and that gathering data should be as targeted as possible.[95]

9. Encryption

The Secretary of State may issue a national security notice to communication service providers that would require them to take steps that are necessary and proportionate in the interest of national security. These notices could require conduct, such as the "provision of services or facilities to assist an intelligence service to carry out its functions more effectively."[96]

The Secretary of State, after consulting with the technical advisory board and any affected communication service provider, would be able to use regulations to impose obligations on communication service providers in the form of technical capability notices to help facilitate assistance in response to warrants under the bill. These obligations could include removing electronic protection to any communications or data.[97] The communications service provider can only be required to remove encryption that it has applied, or that it has had a third party apply on its behalf.[98] Prior to issuing a notice that imposes obligations to remove electronic protection, the Secretary of State must take into account the technical feasibility and cost of compliance.[99] The communications service provider may refer the notice back to the Secretary of State for review, and during this period there is no obligation to comply with the requirements of the notice. During review, the Secretary of State must consult the Technical Advisory Board and Investigatory Powers Commissioner and, after consultation, he or she may then vary, revoke or confirm the notice.[100]

The Investigatory Powers Bill would replace existing provisions, currently contained in the Regulation of Investigatory Powers Act; however, UK technology groups have expressed concerns that clause is unclear as to whether it extends to end-to-end encryption, where the keys are generated for two unique users. TechUK notes that if the provisions of the bill apply to end-to-end encryption it will limit companies' ability to use security to safeguard customers privacy and security, and would result in UK companies having to weaken the security of products in

[93] *Id*. clause 190.

[94] HOUSE OF COMMONS LIBRARY, *supra* note 32, at 52.

[95] Carey, *supra* note 59.

[96] HOUSE OF COMMONS LIBRARY, *supra* note 32, at 69; Investigatory Powers Bill 2015-16, HL Bill 40, clause 2226.

[97] *Id*. and Investigatory Powers Bill, 2015–16, HL Bill 40, clause 217.

[98] *Id*. clause 219.

[99] *Id*. clause 218.

[100] *Id*. clause 220.

order to comply with the legislation.[101] Major technology companies, including Apple, Facebook, Google, Microsoft, Twitter, Yahoo, and Mozilla, have expressed concern that the provisions in the bill would require them to insert "backdoors" into their software to facilitate government access.[102] Concern has also been raised that systems that utilize end-to-end encryption, which service providers currently do not have the capability to decrypt, could be banned in the UK.[103]

10. Offenses

In addition to providing for an authorization mechanism for the lawful interception of communications, the bill also provides for the offenses of unlawfully intercepting or obtaining communications.[104] There are monetary penalties for certain unlawful interceptions.[105] The Bill provides restrictions on authorizing interceptions from overseas authorities as well as under mutual assistance agreements.

The bill imposes a duty, with limited exemptions, not to disclose the existence or details of any warrant or intercepted materials obtained under a warrant. It is an offense to do so.[106] This offense is designed to "prevent the 'tipping-off' of suspects or subjects of interest that their data has been sought, thus informing them that they are under suspicion."[107]

11. Extraterritorial Application

Provisions relating to the interception of communications data would have extraterritorial application, meaning that communications service providers based overseas that handle communications data of citizens of the UK would be covered by the provisions of the Act.[108]

12. Miscellaneous Provisions

In an amendment, the Government Communication Headquarters and Secret Intelligence Service would be allowed to engage in property interference where the property is located in the UK, removing a current restriction that only allows them to undertake activities involving overseas property.[109]

---

[101] HOUSE OF COMMONS LIBRARY, *supra* note 32, at 75.

[102] *Id*.

[103] *Id*.

[104] Investigatory Powers Bill, 2015–16, HL Bill 40 Part I.

[105] *Id*. clauses 3-10.

[106] *Id*. chapter 3.

[107] HOUSE OF COMMONS LIBRARY, *supra* note 32, at 30.

[108] Investigatory Powers Bill 2015-16, HL Bill 40, clauses 81 & 91.

[109] *Id*. clause 224.

13. Oversight

If enacted, the bill would establish an Investigatory Powers Commissioner and Judicial Commissioners to oversee the implementation of legislation. The three Commissioners that currently oversee the use of investigatory powers would be replaced for the first time by an element of judicial oversight. The Judicial Commissioners would be appointed by the Prime Minister after consultation with senior members of the judiciary and must have held high judicial office.[110]

In cases where a public authority commits a serious error and fails to comply with a requirement over which the Investigatory Powers Commissioner has oversight, the Commissioner may inform the individual of the error and his or her right to bring a case to the Investigatory Powers Tribunal.[111]

B. Reaction to the Bill

The only committee that has reviewed the draft bill with full security clearance was the Intelligence and Security Committee, which expressed concern that the bill did not cover all the intrusive capabilities of the intelligence services, leaving some of the powers governed by other legislation, and that privacy protections provided in the bill were inconsistent.[112] The government reportedly responded to these criticisms only by amending the heading of Part I of the bill from "general protections" to "privacy."[113] This response was strongly criticized in both the press and by human rights groups. *The Independent* noted that

> Parliament's Intelligence and Security Committee - the only security-checked committee with access to the most sensitive workings of our intelligence agencies -told [government minister] May to place privacy at the heart of the Bill. Her Home Office officials simply added the word "privacy" to a chapter heading. To treat Parliament with such contempt is beneath one of the great offices of state.[114]

The Times expressed concern that police powers were being coupled with those of the Intelligence Services in the bill, opining that the police, unlike the Intelligence Services, had a long history of exploiting powers that were designed to combat crime for other purposes:[115]

> Britain's security services are known to use their powers discerningly. The same cannot be said about Britain's police. The House of Commons should be wary of gifting them new powers requiring little oversight from anybody other than senior police officers. The

[110] HOUSE OF COMMONS LIBRARY, *supra* note 32, at 61.

[111] *Id.* at 62.

[112] *Id*. at 11.

[113] *Only China and Russia Violate Their Citizens Privacy as Much as the Snoopers' Charter Allows*, THE INDEPENDENT (London) (Mar. 2, 2016), http://www.independent.co.uk/voices/only-china-and-russia-violate-their-citizens-privacy-as-much-the-snoopers-charter-a6907136.html, *archived at* https://perma.cc/4TWV-ZZ24.

[114] *Id.*

[115] HOUSE OF COMMONS LIBRARY, *supra* note 32, at 12.

> home secretary, meanwhile, should not have jeopardised the vital preservation of national security by packaging it alongside new domestic powers that are almost certain to be abused.[116]

The Guardian has expressed concern that digital surveillance powers are being expanded to an uncomfortable level and that the government has made only minimal concessions after the review of the draft bill. It also expressed concern about the burden on communications providers to now automatically keep a year of Internet connection records,[117] and about offenses whose creation was originally justified to tackle terrorism and serious crime being used for other purposes, such as immigration and nationality offenses.[118]

The most heated issues raised by the bill are those of balancing the privacy of individuals and security, concerns of abuse of these inherently intrusive powers, and how much the public should be made aware of the exercise of these powers.[119] Other concerns involve the technology sector, whose cooperation is essential to the successful operation of the Act. The UK's technology industry has raised concerns that the proposed measures may not be feasible to implement, and will have a significant financial impact upon industry and result in a loss of competitiveness in the UK's technology sector. [120] Concerns have also been raised about the cost and security implications of the collection and retention of such large volumes of sensitive data and that the provisions that regulate and govern it are not sufficiently clear, as well as the question of who will bear the costs of the implementation.[121] Given the financial burden on communications service providers that compliance with the provisions in the bill may cause, clause 222 provides that the government would contribute towards any costs incurred when complying with the bill.[122]

---

[116] *Id*. at 12.

[117] *The Guardian View on Surveillance: Keep a Vigilant Eye on the Snoopers*, THE GUARDIAN (London) (Mar. 1, 2016), http://www.theguardian.com/commentisfree/2016/mar/01/the-guardian-view-on-surveillance-keep-a-vigilant-eye-on-the-snoopers, *archived at* https://perma.cc/8CWA-XUPY.

[118] *Id.*

[119] HOUSE OF COMMONS LIBRARY, *supra* note 32, at 61.

[120] *Id.*

[121] *Id.*

[122] *Id*. & Investigatory Powers Bill 2015-16, HL Bill 40, clause 222.

European Union

Theresa Papademetriou
Senior Foreign Law Specialist

SUMMARY Electronic intelligence falls within the domain of the Member States of the European Union (EU), who have sole responsibility for safeguarding their internal security. Electronic surveillance conducted by national law enforcement authorities is inherently linked to the right to privacy and personal data protection. Such rights are enshrined in European Union treaties and secondary legislation as well as in Conventions adopted by the Council of Europe and in the International Covenant on Civil and Political Rights, which binds EU Members. The Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms guarantee the rights to privacy and personal data protection to everyone within the jurisdiction of the EU Member States. Legal issues arising from electronic surveillance that may infringe on the human rights of individuals are not subject to review by the Court of Justice of the EU. Aggrieved individuals, upon exhausting legal remedies at the national level, may bring their cases to the European Court of Human Rights in Strasbourg for a final review.

Following the Snowden revelations in the United States and press reports of mass electronic surveillance conducted by law enforcement authorities of several EU Members, the European Parliament adopted a resolution on the US NSA Surveillance Programme, Surveillance Bodies in Various (EU) Members States and Their Impact on EU Citizens' Fundamental Rights. Moreover, the United Nations General Assembly, in a resolution adopted in 2013, urged UN Members to review their legislation on secret surveillance.

In February 2016, the EU and the United States signed an umbrella agreement on the protection of personal data and privacy for law enforcement purposes.

I. Introduction

Under European Union (EU) treaties, foreign electronic surveillance conducted by national law enforcement authorities of the twenty-eight EU Member States falls within the domain of the EU Members. The Treaty on European Union provides that "national security remains the sole responsibility of each Member State,"[1] and, hence, the EU arguably lacks competence to legislate in this area. Moreover, based on the Treaty on the Functioning of the EU, the Court of Justice of the EU does not have jurisdiction over cases that involve surveillance conducted by national authorities in order to safeguard the internal security of the EU Members.[2]

[1] Consolidated Version of the Treaty on European Union (TEU) art. 4, para. 2, 2016 O.J. (C 202) 1, 13, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2016.202.01.0001.01.ENG&toc=OJ:C:2016:202:TOC#C_2016202EN.01001301, *archived at* https://perma.cc/EY34-D354.

[2] Consolidated Version of the Treaty on the Functioning of the European Union (TFEU) art. 276, 2016 O.J. (C 202) 1, 47, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2016.202.01.0001.01.ENG&toc=OJ:C:2016:202:TOC#C_2016202EN.01004701, *archived at* https://perma.cc/2WJX-NL39.

In conducting electronic surveillance, either foreign or domestic, EU Members are required to maintain a balance between the needs of law enforcement authorities and respect for the fundamental rights to privacy, personal data protection, and private and family life, as such rights are guaranteed in domestic legislation, EU law, and international agreements, including the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHRFF) and the International Covenant on Civil and Political Rights,[3] by which EU Members are bound. Under settled case law of the European Court of Human Rights, national enforcement authorities are required, when conducting electronic surveillance, to justify such activity against the privacy of individuals on the basis of a law that sets forth clearly defined grounds, including national security and public safety, and adheres to the principles of necessity and proportionality.

A number of EU Member States have been identified as engaging in large-scale surveillance. In the aftermath of the Snowden revelations in the United States, it was reported that a number of EU Members, including France,[4] Germany,[5] Sweden,[6] and the United Kingdom,[7] were allegedly involved in mass surveillance operations in cooperation with the United States. The allegations spurred a debate at the EU level with the European Parliament playing a leading role among the EU institutions by instructing the Civil Liberties Committee to conduct an inquiry. The inquiry led to the adoption of the Resolution on the US NSA Surveillance Programme, Surveillance Bodies in Various EU Members States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs.[8]

II. Electronic Surveillance: Competence Issues

Competence in the area of surveillance between the EU and its Member States is delineated in a number of articles found in the Treaty on European Union (TEU) and the Treaty on the Functioning of the EU (TFEU). Article 4, paragraph 2 of the TEU states that the Union "shall

[3] International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, entry into force Mar. 23, 1976, 999 U.N.T.S. 171, https://treaties.un.org/doc/Publication/UNTS/Volume%20999/volume-999-I-14668-English.pdf, *archived at* https://perma.cc/9LKM-LWTU.

[4] Angelique Chrisafis, *France 'Runs Vast Electronic Spying Operation Using NSA-style Methods': Intelligence Agency Has Spied on French Public's Phone Calls, Emails and Internet Activity, Says Le Monde Newspaper*, THE GUARDIAN (July 4, 2013), http://www.theguardian.com/world/2013/jul/04/france-electronic-spying-operation-nsa, *archived at* https://perma.cc/99Q4-9EUJ.

[5] *The German Prism: Berlin Wants to Spy Too*, SPIEGEL ONLINE INTERNATIONAL (June 17, 2013), http://www.spiegel.de/international/germany/berlin-profits-from-us-spying-program-and-is-planning-its-own-a-906129.html, *archived at* https://perma.cc/76UD-VVJT.

[6] Jordan Shilton, *Swedish Intelligence Service Spying on Russia for US National Security Agency*, WORLD SOCIALISTS WEB SITE (Dec. 30, 2013), https://www.wsws.org/en/articles/2013/12/30/swed-d30.html, *archived at* https://perma.cc/8DBJ-FJKA.

[7] *NSA Leaks: UK and US Spying Targets Revealed*, BBC News (Dec. 20, 2013), http://www.bbc.com/news/world-25468263, *archived at* https://perma.cc/MFL9-Y9SJ.

[8] European Parliament Resolution 2013/2188 (INI) of 12 March 2014 on the US NSA Surveillance Programme, Surveillance Bodies in Various EU Members States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0230&language=EN&ring=A7-2014-0139, *archived at* https://perma.cc/X7CF-VSXP.

respect [the Member States'] essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State."[9] In a similar vein, article 72 of the TFEU stipulates that title V of the Treaty pertaining to the Area of Freedom, Security and Justice, "shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security."[10] Moreover, article 73 of the TFEU allows the Member States to "organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between the [competent national agencies] responsible for safeguarding national security."[11]

Whereas electronic surveillance is a state function, as the European Parliament has noted,[12] the EU also possesses some competence concerning the internal security of the EU on the grounds of article 67, paragraph 3 of the TFEU. The article states that the EU "shall endeavor to ensure a high level of security, through measures to prevent and combat crime."[13] The EU has exercised such competence by legislating and concluding international agreements, such as the Terrorist Financing Tracking Programme (TFTP) and Passenger Name Record (PNR) Agreement with the United States,[14] designed to fight terrorism and other forms of serious crime, and by establishing agencies, such as EUROPOL[15] and the Office of the EU Counter-terrorism Co-ordinator, tasked with combating terrorism and organized crime.[16] The Parliament takes the position that the EU enjoys competence in the field of security because of the overlap of the notions of "national security," "internal security," "internal security of the EU," and "international security."[17]

A corollary of the EU's lack of competence in the area of surveillance is its lack of authority to legislate on secret surveillance in order to limit it and/or impose stricter safeguards. In the event that the Commission, using its right of initiative, introduced legislation on the subject, it would not be enforceable given the lack of jurisdiction of the European Court of Justice on security matters.

[9] TEU, *supra* note 1, art. 4, para. 2.

[10] TFEU, *supra* note 2, art. 72.

[11] *Id*.

[12] Resolution 2013/2188 (INI), *supra* note 8.

[13] TFEU, *supra* note 2, art. 67, para. 3.

[14] Press Release, European Commission, EU-US Agreements: Commission Reports on TFTP and PNR (Nov. 27, 2013), http://europa.eu/rapid/press-release_IP-13-1160_en.htm, *archived at* https://perma.cc/7296-YZ3P.

[15] *Europol's Priorities*, EUROPOL, https://www.europol.europa.eu/content/page/europol%E2%80%99s-priorities-145 (last visited Dec. 4, 2014), *archived at* https://perma.cc/SA23-Z4Q4.

[16] *Counter-terrorism Co-ordinator*, COUNCIL OF THE EUROPEAN UNION, http://www.consilium.europa.eu/policies/fight-against-terrorism/eu-counter-terrorism-co-ordinator?lang=en (last visited June 13, 2016), *archived at* https://perma.cc/KSP3-HPWY.

[17] Resolution 2013/2188(INI), *supra* note 8, para. Y.

III. Privacy and Personal Data Protection Issues

Electronic surveillance inevitably involves the collection and storage of personal data, access by law enforcement authorities to such data, and the possible infringement of the rights to privacy and the protection of personal data.

Under EU law, the right to privacy and the right to protection of personal data are two distinct fundamental human rights.[18] These rights are also guaranteed in the legal systems of the EU Member States and in international agreements to which the EU parties are signatories, including the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHRFF).

The Charter of Fundamental Rights of the European Union (CFR), which acquired binding status on December 1, 2009, recognizes the right to privacy in article 7 and the right to the protection of one's personal data in article 8.[19] Furthermore, article 8 reaffirms the principle that personal data must be processed fairly and for specific purposes, based on the consent of the individual concerned or some other legitimate purposes laid down by law. It also recognizes the right of individuals to access the data collected and the right to have it rectified, in case of inaccuracy or incompleteness. Compliance with such rules is entrusted to the control of an independent authority established by the EU Member States.[20] The right to personal data may be restricted by law in order to strike a balance with the freedoms and rights of others and public safety and security, subject to the principle of proportionality, which is established in the EU and in the legal systems of the Member States.[21]

The TFEU recognizes the right of every individual to his/her personal data—that is, individuals own their data.[22] It also introduced a new and specific legal basis for the adoption of rules on data protection and granted authority to the EU legislative bodies (Parliament and Council) to adopt rules concerning the processing of personal data in the field of judicial cooperation in

[18] The right to privacy is also protected by article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHRFF), CETS No. 005 (1950), http://www.echr.coe.int/Documents/Convention_ENG.pdf, *archived at* https://perma.cc/S63S-8ZZF, to which all EU Member States are states parties, as members of the Council of Europe. In addition, automatic processing of personal data is protected and governed by the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data and Its Protocol, ETS No. 108 (1981). *Details of Treaty No. 108*, COUNCIL OF EUROPE, http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm (last visited June 14, 2016), *archived at* https://perma.cc/C259-ARSZ. Recently, the Council of Europe began revising the 1981 Convention to bring it in line with contemporary technology and ensure harmonization with EU legal reforms. The Consultative Committee of the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (ETS No. 108), *Modernization of Convention 108: New Proposals* (Mar. 5, 2012), http://www.coe.int/t/dghl/standardsetting/dataprotection/tpd_documents/T-PD-BUR_2012_01Rev_en.pdf, *archived at* https://perma.cc/C6EU-SASH.

[19] Charter of Fundamental Rights of the European Union, 2016 O.J. (C 202/2) 389, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2016:202:TOC, *archived at* https://perma.cc/F9DE-FEKD.

[20] *Id*. art. 8.

[21] *Id.* art. 52(1).

[22] TFEU, *supra* note 2, art. 16.

criminal matters, and police cooperation in the cross-border and domestic processing of personal data.[23]

The right to respect for private and family life, home, and correspondence is established in article 8 of the ECHRFF, to which all EU Members are also participating states as members of the Council of Europe.[24] The ECHRFF recognizes, however, that there are circumstances in a democratic society where it may be necessary for the state to interfere with this right, but only in accordance with the law and for certain clearly defined grounds, such as national security, public safety, economic well-being, the prevention of crimes, and the protection of the rights and freedoms of others.[25] When such interference by public authorities acting in their official capacities does occur, article 13 of the ECHRFF requires a means of redress for the affected individual.[26]

A. Directive 95/46/EC on Personal Data Protection

Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data is the basic framework legislation in the EU on personal data protection.[27] The Directive provides strong protections applicable to the processing of personal data of persons living within the jurisdiction of the EU Member States. Pursuant to Directive No. 95/46/EC on personal data protection, the ownership of personal data belongs to individuals who have legal rights over the collection and processing of personal data. One of the key requirements for the processing of personal data is that the data subject must unambiguously give his/her consent, after being informed that his/her data will be processed.

Pursuant to the Directive, the data subject has the right of access, as provided for in article 12, which means that the data subject is entitled to information regarding any processing of his/her data, the purposes of processing, the categories of the data, and the recipients of the data.[28] The basic principles governing the processing of one's personal data are the following:

- Finality: Data must be collected for an explicit, specific, and legitimate purpose.
- Transparency: Individuals must be informed of the data collected and the purpose of collection.
- Legitimacy: Processing must be occur for a legitimate reason pursuant to article 7 of the Directive.

---

[23] *Id*. art. 16, para. 2.

[24] ECHRFF, *supra* note 18, art. 8.

[25] *Id*. art. 8.

[26] *Id*. art. 13.

[27] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML, *archived at* https://perma.cc/5R5E-CHFB.

[28] *Id*. art. 12.

- Proportionality: The personal data collected must be adequate, relevant, and not excessive in relation to the purpose of collection.
- Accuracy and Retention of the Data: Individuals' records must be accurate and up to date. False or inaccurate data must be corrected.

Directive 95/46/EC will be repealed on May 25, 2018, and replaced by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).[29] Regulation 2016/679 will be applicable as of May 25, 2018.[30]

In addition to the above Regulation, the EU adopted Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA.[31] Member States have an implementation deadline of May 6, 2018, to comply with this Directive.[32]

Intelligence activities conducted by national law enforcement authorities that involve national security issues or issues concerning the common foreign and security policy of the EU fall outside the scope of Regulation 2016/679 and Directive 2016/680.[33]

B. Confidentiality of Communications

Confidentiality of communications is a principle enshrined in the legal systems of the EU Member States. At the EU level, confidentiality of communications is stipulated in Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications).[34] In

[29] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) art. 94, 2016 O.J. (L 119) 1, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016R0679, *archived at* https://perma.cc/3DBH-PKN4.

[30] *Id*. art. 99.

[31] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 119) 89, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016R0679, *archived at* https://perma.cc/BH32-VK2P.

[32] *Id*. art. 63.

[33] *Id*. Preamble (16).

[34] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) art. 5, 2002 O.J. (L 201) 37, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML, *archived at* https://perma.cc/AFB3-JCPU.

particular, article 5 of the Directive requires that EU Members "prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than the users, without the consent of the users concerned, except when legally authorized to do so in accordance with article 15(1)."[35]

C. Exemptions

Interception or surveillance is permitted on the grounds of national security; defense and public security; and the prevention, investigation, detection, and prosecution of criminal offenses or of unauthorized use of an electronic communications system, as referred to in article 13(1) of Directive 95/46/EC.[36]

EU Members are also allowed to adopt legislation on data retention for a limited period and based on the same grounds provided above.[37]

D. Data Retention

Prior to its invalidation in April 2014, Directive No. 2006/24/EC (the Data Retention Directive),[38] required the providers of publicly available electronic communications services or public communications networks to retain traffic and location data belonging to individuals or legal entities. Such data included the calling telephone number and name and address of the subscriber or registered user, user IDs (a unique identifier assigned to each person who signs with an electronic communications service), Internet protocol addresses, the numbers dialed, and call forwarding or call transfer records. The retention period was to last for a minimum period of six months and up to two years, and the sole purpose of processing and storing the data was to prevent, investigate, detect, and prosecute serious crimes, such as organized crime and terrorism. The content of the communications of individuals was not retained.

On April 8, 2014, the Grand Chamber of the Court of Justice of the European Union (CJEU) issued a judgment declaring the Directive invalid.[39] The Directive was challenged on the grounds of infringement of the right to private life, and the right to the protection of personal data of individuals, as guaranteed in articles 7 and 8, respectively, of the Charter of Fundamental Rights of the European Union.

---

[35] *Id*. art. 5(1).

[36] *Id*. art. 15(1).

[37] *Id*.

[38] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 54, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF, *archived at* https://perma.cc/BVQ3-ZSR5.

[39] Grand Chamber, Digital Rights Ireland Ltd. (C–293/12) v. Minister for Communications, Marine and Natural Resources (Apr. 8, 2014), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293, *archived at* https://perma.cc/A5DF-ZJF2.

In examining the issue of interference with the rights to privacy and the protection of personal data, the CJEU made the following observations:

- The obligation imposed on providers of electronic communications services or public communications networks "constitutes in itself an interference with the rights guaranteed by article 7 of the Charter,"
- Access of the national authorities to data "constitutes a further interference with that fundamental right," and
- The interferences described above also violate the right to protection of personal data.[40]

The CJEU reasoned that the Directive did not establish clear and precise rules that regulate the "extent of interference with the fundamental rights of Art. 7 and 8 of the Charter."[41] Therefore, it concluded that the Directive "entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary."[42]

The CJEU also held that the security and protection of personal data cannot be fully guaranteed in the absence of review of compliance by an independent authority of the rules on data protection, as required by article 8 of the Charter of Fundamental Rights.[43]

In September 2015, the Commission announced that, following the CJEU's decision, it has no plans to introduce new legislation on data retention at the EU level. Therefore, EU Members are free to adopt national rules on this issue.[44]

E. EU–US Agreement

On June 2, 2016, the European Union and the United States signed the Agreement on the Protection of Personal Data Information Relating to the Prevention, Investigation, Detection and, Prosecution of Criminal Offenses.[45] The Agreement covers all personal data, such as names, addresses, and criminal records that will be exchanged between the EU and the US for the purposes of the prevention, detection, investigation, and prosecution of criminal offenses, including terrorism.[46] In addition, the Agreement will provide safeguards and guarantees the

[40] *Id*. paras. 34–36.

[41] *Id*. para. 65.

[42] *Id*.

[43] *Id*. para. 66.

[44] Press Release, European Commission Statement on National Data Retention Laws (Sept. 16, 2015), http://europa.eu/rapid/press-release_STATEMENT-15-5654_en.htm, *archived at* https://perma.cc/MT7Y-EL9M.

[45] *Signing of the "Umbrella" Agreement: A Major Step Forward in EU-U.S. Relations*, EUROPEAN COMMISSION, JUSTICE (June 2, 2016), http://ec.europa.eu/justice/newsroom/data-protection/news/160602_en.htm, *archived at* https://perma.cc/5Q47-WFDD.

[46] Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses (Draft for

lawfulness of data transfers, and will improve and facilitate EU–US law enforcement cooperation. The Agreement will enter into force one month after both parties exchange notifications that their domestic ratification procedures have taken place.[47] At the EU level, the European Parliament must give its consent to conclude the Agreement.

IV. Case Law

A. Jurisdiction

Legal challenges to intelligence operations on the grounds of infringing the rights of the individual (such as the right to privacy freedom of expression, and a remedy) or because the intelligence operations are not conducted in accordance with the applicable law and are in violation of the standards of necessity and proportionality are not subject to review by the Court of Justice of the EU, as explicitly stated in article 276 of the TFEU:

> in exercising its powers regarding the provisions of Chapters 4 and 5 of Title V of Part Three relating to the area of freedom, security and justice, the Court of Justice of the European Union shall have no jurisdiction to review the validity or proportionality of operations carried out by the police or other law enforcement services of a Member State or the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security.[48]

Such challenges can be brought before the European Court of Human Rights (ECHR), however. In general, the ECHR has found that the "mere existence of legislation allowing secret surveillance constitutes an interference with private life such that the necessity and legality requirements of article 8 of the European Convention on Human Rights must be met."[49] The ECHR has also found that emails, telephone communications, faxes, and Internet usage fall within the ambit of article 8 of the Convention.[50]

As far as the legality requirement, the ECHR has a strict requirement that surveillance activities must be based on a law and not conducted as matter of policy.[51]

Initialing) art. 3. http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf, *archived at* https://perma.cc/FXY5-3NAP.

[47] *Id*. art. 29.

[48] TFEU, *supra* note 2, art. 276.

[49] SARAH ST. VINCENT, CENTER FOR DEMOCRACY & TECHNOLOGY, INTERNATIONAL LAW AND SECRET SURVEILLANCE: BINDING RESTRICTIONS UPON STATE MONITORING OF TELEPHONE AND INTERNET ACTIVITY 9 (SEPT. 4, 2014) (CITING WEBER & SARAVIA V. GERMANY (2006), https://cdt.org/files/2014/09/CDT-IL-surveillance.pdf, *archived at* https://perma.cc/2TGV-HUBD.

[50] Grand Chamber, Digital Rights Ireland Ltd. (C–293/12), at 9.

[51] *Id*. at 10.

B. Case of Szabo and Vissy v. Hungary

In January 2016, the ECHR issued a critical judgment on mass surveillance issues in the case of *Szabo and Vissy v. Hungary*.[52] Two applicants challenged 2011 legislation that permitted broad surveillance activities of the Hungarian Anti-Terrorism Task Force, on the grounds that it violated the applicants rights to privacy, home, and correspondence. The ECHR ruled against Hungary because the contested legislation violated the rights of the applicants, due to sweeping secret surveillance, the lack of notification of surveillance measures, and other effective safeguards.[53] As far as *ex ante* (prior) authorization, the ECHR held that it is not mandatory, as long as there is *ex post* judicial control. However, the ECHR ruled that Hungary failed to meet this requirement as well.[54]

The ECHR has developed a number of minimum standards to which the national laws of the Member States of the Council of Europe must adhere, in order to avoid abuses of power and future litigation by affected or concerned individuals. [55] These standards include: (a) a description of the nature of the offenses that may give rise to an interception order; (b) identification of the categories of people who are likely to have their telephones tapped; (c) a limit on the duration of telephone tapping; (d) the procedure to be followed for examining, using, and storing the data obtained; (e) the precautions to be taken when communicating the data to other parties; and (f) the circumstances in which recordings may or must be erased or the tapes destroyed.[56]

A decision to authorize surveillance activity must be given by an independent body prior to initiation of such activities; it is not necessary that the body that gives authorization is judicial as long as it enjoys independence from the executive.[57] The ECHR has accepted the practice of governments to waive authorization in emergency situations in order to expedite an operation, or where, due to the circumstances, authorization is not possible.[58]

As the ECHR has emphasized, especially in cases where prior authorization is not possible, the *ex post* review of government surveillance, either judicial or otherwise, is absolutely essential.[59] That oversight, which must be performed by an independent external body, is also recommended by the UN Rapporteur on Human Rights. In its 2010 Report on Compilation of Good Practices on Legal and Institutional Frameworks and Measures that Ensure Respect for Human Rights by Intelligence Agencies While Countering Terrorism, Including on Their Oversight, the UN

[52] Case of Szabó and Vissy v. Hungary, App. No. 37138/14 (Eur. Ct. H.R., Jan. 12, 2016), http://hudoc.echr.coe.int/eng?i=001-160020, *archived at* https://perma.cc/69PE-HLFZ.

[53] *Id*. para. 89.

[54] *Id*. para. 56.

[55] *Id*. paras. 57 & 72.

[56] *Id*. para. 56.

[57] *Id*. para. 77.

[58] *Id*.

[59] *Id*. paras. 77 & 80.

Rapporteur suggested that oversight be exercised by at least one institution fully independent of both the intelligence services and the political executive.[60]

Finally, an individual must be provided with an effective remedy through an existing complaint mechanism where one may raise allegations of violations of privacy rights.[61]

V. Large-scale Surveillance and Compatibility with Human Rights

As stated above, at the EU level, large-scale surveillance conducted by government agencies of the EU Member States has raised concerns as to the compatibility of such activities with human rights standards.

The Parliament's Resolution on the US NSA Surveillance Programme, Surveillance Bodies in Various EU Members States and Their Impact on EU Citizens' Fundamental Rights, mentioned above,[62] is a political statement lacking binding force. It urged EU Members to discontinue the mass collection of data and to ensure that national laws and policies on electronic surveillance are in line with EU and Council of Europe standards. It also proposed to establish at the EU level a high-level group to monitor progress. In April 2014, the Parliament also requested the EU Agency for Fundamental Rights (FRA) to conduct research on the impact of large-scale surveillance on fundamental rights and to review whether individuals whose data are collected by intelligence agencies have adequate remedies against such practices. The FRA's final report will be published in 2017.[63]

Similarly, the United Nations General Assembly adopted a resolution on December 18, 2013, urging UN Members to respect the right of privacy in digital communications and to review their legislation and practices on secret surveillance.[64]

A 2013 study conducted by the Directorate General for Internal Policies of the European Parliament, entitled *National Programs of Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law*, examines mass surveillance practices in four EU countries: France, Germany, Sweden, Netherlands, and the United Kingdom.[65] The study

---

[60] Martin Scheinin, Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, *Compilation of Good Practices on Legal and Institutional Frameworks and Measures that Ensure Respect for Human Rights by Intelligence Agencies While Countering Terrorism, Including on Their Oversight*, at 9, U.N. Doc. A/HRC/14/46 (May 17, 2010), https://fas.org/irp/eprint/unhrc.pdf, *archived at* https://perma.cc/JR29-GU86.

[61] *Id*. paras. 77, 78 & 80.

[62] Resolution 2013/2188(INI), *supra* note 8.

[63] *National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies*, EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, http://fra.europa.eu/en/project/2014/national-intelligence-authorities-and-surveillance-eu-fundamental-rights-safeguards-and (last visited June 14, 2016), *archived at* https://perma.cc/DW2E-EMD2.

[64] The Right to Privacy in the Digital Age, G.A. Res. 68/167, U.N. Doc A/RES/68/167 (Dec.18, 2013), http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167, *archived at* https://perma.cc/HAY5-TFXJ.

[65] EUROPEAN PARLIAMENT DIRECTORATE GENERAL FOR INTERNAL POLICIES, NATIONAL PROGRAMMES FOR MASS SURVEILLANCE OF PERSONAL DATA IN EU MEMBER STATES AND THEIR COMPATIBILITY WITH EU LAW (hereinafter

indicates that cooperation with foreign intelligence services appears to be a common practice. The study cites the so-called "Five Eyes" network, which comprises the US, UK, Canada, Australia, and New Zealand, that originated from a 1946 multilateral agreement for cooperation in signals intelligence, and which has extended over time in terms of activities (Echelon, and now Fornsat).[66] The US also engages in cooperative relationships with "second-tier" and "third-tier" partners such as France and Germany.[67]

The report indicates that some legal regimes operate on the basis of orders issued by special courts (for instance, in Sweden), while others were based on warrants issued by the government (the UK and Netherlands) or through an authorization role accorded to specially appointed oversight bodies (Germany, France, and Netherlands).[68]

With regard to oversight, the report found that in several Member States oversight bodies encounter a number of constraints that limit their ability to scrutinize the intelligence agencies' surveillance practices. In Sweden, the two main oversight institutions—the intelligence court and the Statens inspektion för försvarsunderrättelseverksamheten (Siun, State Inspection for Defense Intelligence Activity)—are deemed to be insufficiently independent. France's main oversight body, the Commission nationale pour les interceptions de securité (CNCIS, National Commission for Security Interceptions), was found to be substantially constrained in its reach, because it has limited administrative capacity. The report also identified gaps in the UK's intelligence oversight regime, as evidenced by the statement released in July 2014 by the Intelligence Security Committee on the Government Communications Headquarters' (GCHQ's) alleged interception of communications under the PRISM program.[69]

The report also found that the surveillance programs operated by the Member States endanger the EU principle of "sincere cooperation," enshrined in article 4.3 of the Treaty on the European Union, because they compromise compliance with existing EU-level mutual assistance and cooperation legal regimes and lawful searches between EU Member States and with the US, and also compromise the internal security of the EU.

MASS SURVEILLANCE STUDY) 24 (Oct. 2013), http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf, *archived at* https://perma.cc/7X8D-WAV9.

[66] For more information on on surveillance, including Echelon/Fornsat, see EUROPEAN PARLIAMENT, INTERCEPTION CAPABILITIES 2014, http://www.europarl.europa.eu/document/activities/cont/201309/20130916ATT71388/20130916ATT71388EN.pdf, *archived at* https://perma.cc/JW6E-PK59.

[67] MASS SURVEILLANCE STUDY, *supra* note 65, at 24.

[68] *Id*. at 25.

[69] *Id*. at 26.