Model Courts of Justice 2022

European Court of Human Rights

Study Guide

WRITTEN BY HAZAL AKIN
ASSISTED BY YAĞMUR ÇİÇEK
SUPERVISED BY ZEYNEP GÜLER

LETTER OF THE SECRETARY-GENERAL

Most Esteemed Participants,

On behalf of our academic and organization teams, once again I would like to welcome you to the Model Courts of Justice Family as The Secretary-General of the Model Courts of Justice Conference 2022! My name is Zeynep Güler, and I am a junior at Ankara University, Faculty of Law.

In this court we will be examining the nature and vastness of internet surveillance under the scope of 'Data Protection', which will be seamlessly connecting our participants with the legal world and its concepts. Supported by the agenda of data privacy, which is a very controversial topic in the world of today, I have no doubt that every participant of the European Court of Human Rights will enjoy Model Courts of Justice 2022 to the fullest.

This Study Guide was prepared by two graceful ladies Ms Hazal Akın and Academic Asisstant Ms Yağmur Çicek. Writing an agenda item for such a key committee is no easy task, but from the moment they joined this team, I had no doubt that the ECHR would live up to all expectations. Therefore, I have to thank them once again for being a part of this team and for working tirelessly to achieve perfection.

Before attending our court sessions, I strongly advise all participants to read the Study Guide, the Handbook, the Rules of Procedure, and any other documents available on our website. If you have any queries about the conference or the committee, please do not hesitate to contact me at secretarygeneral@modelcj.org.

Sincerely,

Zeynep GÜLER

Secretary-General of Model Courts of Justice 2022

LETTER OF THE UNDER-SECRETARY-GENERAL

Dear Participants,

I am delighted to welcome you to the eleventh annual session of Model Courts of Justice 2022. My name is Hazal Akın and I am a senior student at Ankara University, Faculty of Law. This year, I have the special honour of serving you as the Under-Secretary-General responsible for the European Court of Human Rights.

This year's session, European Court of Human Rights will hear a landmark case concerning the legitimacy of mass surveillance system under the European Convention on Human Rights. The case, namely Big Brother Watch v UK will offer invaluable experience in dealing with the bulk interception of communications and related communications data, addressing the most intrusive aspects of surveillance practices, and the legal quality of being claimable of information gathered by foreign intelligence services.

I would want to express my gratitude to our Secretary-General, Ms. Zeynep Güler, for presenting me with this precious opportunity and for her in-depth guidance, unwavering support, and patience throughout the entire process. I would also like to convey my gratefulness to my assistant Ms. Yağmur Çiçek for her diligent work and my colleagues for their devoted efforts and contribution to the academic process. Moreover, I would like to thank to our Director-General, Ms. Başak Göksu, and her team for once again demonstrating organizational excellence via their hard work and dedication.

If you have any questions, please do not hesitate to contact me.

Hazal Akın

Under-Secretary-General responsible for the European Court of Human Rights

LETTER OF THE ASSISTANT TO THE SECRETARY-GENERAL

Dear Participants,

First of all, I would like to welcome you to the eleventh edition of our conference, Model Courts of Justice 22! My name is Yağmur Çiçek, and I am a junior at Ankara University, Faculty of Law. This year, it will be a pleasure to serve you as Assistant to the Secretary-General.

This year, the Model Courts of Justice will go back in time to simulate one of the notable cases in the European Courts of Human Rights, which is named Big Brother Watch v. The United Kingdom. I am delighted to have been involved in the creation of the study guide for this case, which has a large-scale impact and covers a variety of subjects, including over intelligence sharing, and the bulk interception of communications.

I would like to offer my sincere thanks to the Under-Secretary General Ms. Hazal Akın, with whom I have enjoyed working with for preparing this remarkable case. Furthermore, I would like to express my gratitude to our honourable Secretary-General Ms. Zeynep Güler for her endless support and my dearest friends from the academic team for their great efforts through this academic year. Lastly, I would like to thank Director-General Ms. Başak Göksu and our organization team led by her for greatly handling the organizational matters and making sure everything is running perfectly.

If you have any questions, please do not hesitate to contact me.
Yağmur ÇİÇEK
Assistant to the Secretary-General

TABLE OF CONTENTS

I. INTRODUCTION TO THE EUROPEAN COURT OF HUMAN RIGHTS

The European Court of Human Rights (ECHR) is a regional human rights judicial body that was established under the auspices of the Council of Europe and is situated in Strasbourg, France. Since its establishment in 1959, the European Court of Human Rights has issued over 10,000 decisions on alleged violations of the European Convention on Human Rights.[1]

The European Commission on Human Rights was a foundation that had previously evaluated the admissibility of complaints, supervised friendly settlements, and referred some cases to the Court. With the arrangements established in 1998, it was abolished, and the right of individual application was made mandatory, allowing individuals to apply to the Court directly if they believe their human rights have been violated.[2] Thereby, the European Court of Human Rights became a single, full-time court as a result of this arrangement. Because of these features, this court has gained much importance and its applications are increasing with each passing day.[3]

1. History

While ideas of a peaceful world order have existed for centuries, the twentieth century witnessed more forceful movements toward organizations that aim to achieve peace through law. [4] One of the key steps was the establishment of the Council of Europe in 1949 with the aim of *'to achieve a greater unity between its Members for the purpose of safeguarding and realizing the ideals and principles which are their common heritage and facilitating their economic and social progress.'*, according to Article 1 of the Statute of the Council of Europe.[5]

Subsequently, the Convention for the Protection of Human Rights and Fundamental Freedoms, commonly known as the European Convention on Human Rights, was signed on November 4, 1950, in Rome, and went into force on September 3, 1953.[6] It was developed to

[1] (*Ijrcenter.org*, 2022) <https://ijrcenter.org/european-court-of-human-rights/> accessed 8 March 2022.
[2] Ibid.
[3] 'A Brief History Of The European Court Of Human Rights - Eachother' (*EachOther*, 2022) <https://eachother.org.uk/brief-history-european-court-human-rights/> accessed 10 March 2022.
[4] Stephanie Schmahl and Marten Breuer, *The Council Of Europe Its Law And Policies* (1st edn, Oxford University Press 2017) p.3
[5] Stephanie Schmahl and Marten Breuer, *The Council Of Europe Its Law And Policies* (1st edn, Oxford University Press 2017) p.28
[6] (*Echr.coe.int*, 2022) <https://www.echr.coe.int/Documents/50Questions_ENG.pdf> accessed 10 March 2022.

ensure that governments would never again be permitted to dehumanize and abuse the rights of the people, and to help realize the promise of 'never again'.[7]

Image: European Court of Human Rights (Strasbourg, 1994)[8]

The European Court of Human Rights was formed on January 21, 1959, with a mandate that was situated under Article 19 of the European Convention on Human Rights to verify that States that signed up to the European Convention on Human Rights fulfilled their obligations. The first members of the court were appointed by the Parliamentary Assembly of the Council.[9]

The European Convention on Human Rights has undergone various revisions over the years, which were enforced through the adoption of additional protocols; it now includes 11 additional protocols. On November 1, 1998, when Protocol No.11 to the convention entered into force, it was especially notable among these many instruments as it resulted in a considerable simplification of the European human rights regime. The agreement united two of the enforcement mechanisms of the convention, the European Commission on Human Rights and the European Court of Human Rights, into a reconstituted court, which is now able to examine individual applications.[10]

Individuals did not have direct access to the European Court of Human Rights until this protocol became effective, they had to first apply to the Commission. In addition, if the commission finds the case to be well-founded, it will bring a case on behalf of the individual in

[7] 'What Is The European Convention On Human Rights?' (*Amnesty.org.uk*, 2022) <https://www.amnesty.org.uk/what-is-the-european-convention-on-human-rights> accessed 10 March 2022.
[8] 'European Court Of Human Rights (Strasbourg,1994)' <https://structurae.net/en/structures/european-court-of-human-rights> accessed 30 March 2022.
[9] 'A Brief History Of The European Court Of Human Rights - Eachother' (*EachOther*, 2022) <https://eachother.org.uk/brief-history-european-court-human-rights/> accessed 15 March 2022.
[10] 'European Convention On Human Rights | Summary, History, & Facts' (*Encyclopedia Britannica*, 2022) <https://www.britannica.com/event/European-Convention-on-Human-Rights-Europe-1950> accessed 10 March 2022.

court. This issue was avoided with the implementation of this protocol, and individuals were allowed to apply directly to the court.[11]As a result, in addition to establishing a catalogue of civil and political rights and freedoms, the Convention also established a mechanism for the enforcement of the responsibilities of the Contracting States.[12]

Even into the late 1980s, the Court was generally quiet with 1009 applications filed in 1988. With more than 90% of the judgments of the Court delivered between 1998 and 2008, over 50,000 applications were filed with the Court.[13] The entry into force of Protocol 11 in 1998 had a huge impact on the number of cases that were brought before the Court. For individuals who claim their human rights have been violated, it made the right to file an individual application mandatory. Therefore, the number of applications to this judicial body, which was established to ensure the implementation of the European Convention on Human Rights, is increasing.[14]

Signatories to the Convention are obligated to protect a variety of civil and political rights, including freedom of expression and religion, the right to a fair trial and data privacy. As an example, Article 8 of the Convention governs the protection of personal data and considers that everyone has the right to respect for their private and family lives, their home and their correspondence. The Court has considered a large number of personal data transactions carried out by the competent authorities or other private entities and has evaluated in this context whether the rights of the persons concerned have been violated in the scope of Article 8.[15] Therefore, it appears that the intervention of the European Court of Human Rights and the use of the jurisdiction of the court in disputes arising from the breach of these rules has become more necessary to protect human rights and fundamental freedoms.[16]

2. Structure

[11] 'European Human Rights System - Research Guides' (*Library.law.columbia.edu*, 2022) <http://library.law.columbia.edu/guides/European_Human_Rights_System#The_European_Human_Rights_System._The_Commission_of_Human_Rights._How_to_Find_a_Report_of_the_Commission> accessed 20 March 2022.

[12] (*Rechtspraak.nl*, 2022) <https://www.rechtspraak.nl/SiteCollectionDocuments/European-court-of-human-rights.pdf> accessed 13 March 2022.

[13] 'A Brief History Of The European Court Of Human Rights - Eachother' (*EachOther*, 2022) <https://eachother.org.uk/brief-history-european-court-human-rights/> accessed 15 March 2022.

[14] A. H. Robertson, 'The European Court of Human Rights' (1960) 9 Am J Comp L 1 p.1

[15] Council of Europe, 'Guide To The Case-Law Of The European Court Of Human Rights- Data Protection' (2021) p.31

[16] A. H. Robertson, 'The European Court of Human Rights' (1960) 9 Am J Comp L 1 p.1

In order to handle a large number of cases simultaneously, the court is separated into five sections, or administrative bodies, each with its own judicial chamber. A President, Vice President, and a number of judges are appointed to each part.[17]

Section II of the European Convention on Human Rights contains the provisions governing the structure and procedure of the Court. The number of judges on the Court is equal to the number of contracting states, and the current number is 47. Judges are chosen by the Parliamentary Assembly of the Council of Europe, which votes on a list of three candidates proposed by governments. Judges are chosen for a six-year term, and they can be re-elected. Their terms of duty finish when they reach the age of seventy, but they continue to work on cases that have already been assigned to them. Besides that, judges serve on the Court in their individual capacities, not as representatives of any state. They are prohibited from engaging in any activity that would threaten their independence or impartiality.[18]

The judges of the Court work in four separate judicial formations to which the applications are allocated.[19]

• Single Judge: Based on the information provided by the applicant, the judge may only rule on the validity of applications that are clearly unacceptable.

• Committee: It is composed of three judges who make decisions on the admissibility and merits of cases involving issues covered by well-developed case law, and their decisions are unanimous.

•Chamber: It is made up of seven judges who rule on admissibility and merits for cases that have caused problems and have yet to be resolved, and a decision can be made by a majority. Chambers determine the great majority of the decisions of the Court.[20] Each chamber also has the Section president and the national judge, who have the nationality of the State against which the application is filed.

• Grand Chamber: Consisting of 17 judges, it hears a small number of cases referred to it by an appeal from a chamber decision or abandoned by a chamber when the matter involves a significant or unusual issue. The Grand Chamber never accepts applications directly. The President and Vice-President of the Court, the five Section presidents, and the national judge are always present in the Grand Chamber.

[17] (*Ijrcenter.org*, 2022) <https://ijrcenter.org/european-court-of-human-rights/> accessed 11 March 2022.
[18] (*Rechtspraak.nl*, 2022) <https://www.rechtspraak.nl/SiteCollectionDocuments/European-court-of-human-rights.pdf> accessed 13 March 2022.
[19] (*Ijrcenter.org*, 2022) <https://ijrcenter.org/european-court-of-human-rights/> accessed 11 March 2022.
[20] (*Rechtspraak.nl*, 2022) <https://www.rechtspraak.nl/SiteCollectionDocuments/European-court-of-human-rights.pdf> accessed 13 March 2022.

3. Proceedings Before the Court

The majority of judicial proceedings are handled in writing, and public sessions are rare. There is no fee for submitting an application, and the applicant may request legal aid to cover costs incurred later in the process. While lawyers are not necessary to file a complaint, they are required to represent the applicant at any hearing before the Court once the application is confirmed to be admissible.[21]

In analysing cases submitted before the court, there are two basic steps. The admissibility step is the first of these stages, and it determines whether the matter can be examined by the court. The major step, where the concerns are examined, is the second stage.[22] The speed and duration of the proceedings will be determined by the nature of the case.[23]

a. Admissibility

When the Court receives an application, it must determine if it fulfils all the standards for admissibility. A single judge, a three-judge committee, or a seven-judge chamber can make an admissibility determination. An application must meet the following requirements to be declared admissible:

- The use of all household remedies has been exhausted.
- Applications must be submitted within four months from the final domestic judicial decision.
- A complaint brought against a signatory to the European Convention on Human Rights.
- The applicant was at a significant disadvantage.

If an application fails to meet any of these criteria, it will be ruled inadmissible and will not be examined for further consideration.[24] Inadmissibility decisions, as well as judgments taken by Committees and Grand Chambers, are final and cannot be appealed.[25]

b. Merits

[21] *(Ijrcenter.org*, 2022) <https://ijrcenter.org/european-court-of-human-rights/> accessed 16 March 2022.
[22] (*Echr.coe.int*, 2022) <https://www.echr.coe.int/Documents/50Questions_ENG.pdf> accessed 11 March 2022.
[23] *(Ijrcenter.org*, 2022) <https://ijrcenter.org/european-court-of-human-rights/> accessed 11 March 2022.
[24] *(Ijrcenter.org*, 2022) <https://ijrcenter.org/european-court-of-human-rights/> accessed 16 March 2022.
[25] (*Echr.coe.int*, 2022) <https://www.echr.coe.int/Documents/50Questions_ENG.pdf> accessed 14 March 2022.

If there is no problem with admissibility in the application, the issue is allocated to one of the five divisions of the ECHR, and the complaint is sent to the opposing State. Following that, both parties have the opportunity to offer their findings to the Court, which may contain specific information requested by the Head of the Chamber or Division, as well as any other materials deemed relevant to the case by the parties. The court that will hear the case has the option of deciding on admissibility and merits separately, or it can decide on both if it notifies the parties.[26]

Within three months of receiving the judgment of the Chamber, the parties to the dispute may request that the case be sent to the Grand Chamber for reconsideration. Requests for referral to the Grand Chamber are reviewed by a panel of judges, which determines whether the referral is suitable.[27]

Judgments finding violations bind the states involved, and they are required to carry them out. The Committee of Ministers of the Council is in charge of overseeing the execution of judgments, especially ensuring that the amounts awarded by the Court to the applicants in compensation for damages they have suffered are paid.[28] This also includes reasonable satisfaction or monetary compensation, which is known as 'just satisfaction', when a court rules against a state and finds that the applicant was harmed.[29]

c. Friendly Settlements

A friendly settlement is a compromise made by the disputing parties to bring the case to a conclusion. As a result, the parties avoid a win–lose situation in their dispute, and both parties' benefit. The procedure is based on principles of international law for resolving peaceful conflicts. It is also a reflection of the subsidiarity principle, which states that it is their obligation to protect human rights first and foremost, and to provide remedies consequently.[30]

Article 39(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms lays the foundation for peaceful settlements. It is stated that *'At any stage of the proceedings, the Court may place itself at the disposal of the parties concerned with a view to securing a friendly settlement of the matter on the basis of respect for human rights as defined*

[26] *(Ijrcenter.org*, 2022) <https://ijrcenter.org/european-court-of-human-rights/> accessed 16 March 2022.
[27] (*Echr.coe.int*, 2022) <https://www.echr.coe.int/Documents/50Questions_ENG.pdf> accessed 14 March 2022.
[28] Ibid.
[29] Octavian Ichim, *Just Satisfaction Under The European Convention On Human Rights* (1st edn, Cambridge University Press 2015) p.11
[30] Octavian Ichim, *Just Satisfaction Under The European Convention On Human Rights* (1st edn, Cambridge University Press 2015) p.181

in the Convention and the Protocols thereto.' The friendly settlement procedure of the Convention allows the parties to resolve a dispute, usually in exchange for the payment of a specified sum of money by the respondent party to the applicant or an undertaking by the respondent party to provide an appropriate resolution of the issue or both.[31] However, the negotiations for a friendly settlement will be kept confidential and will not affect the arguments of the parties in the contentious proceedings.[32]

The friendly settlement procedure of the European Court of Human Rights is an important tool for reducing the workload of the Court. Given that the Court does not usually prescribe appropriate remedies or secure other sorts of compensation, a settlement, particularly for the applicant, has the potential to result in faster justice than usual. Given the advantages of this method for both the court and the parties, the court has announced that it intends to increase the number of cases closed by friendly settlements in 2018.[33]

When a friendly settlement is reached, the issue is removed from the list of the Court, and a brief statement about the remedies is shared with the public. This decision will then be submitted to the Committee of Ministers, which is in charge of overseeing the implementation of the terms of the friendly settlements. If the parties are unable to reach an agreement, the Court will continue with the case and make a judgment on the merits.[34]

d. Interim Measures

Interim measures are emergency measures only applicable when irreparable harm is threatened, according to the well-established practice of the Court. Such measures are decided as part of the proceedings of the Court, without prejudice to any subsequent decisions on the admissibility or merits of the matter.[35] These measures generally involve asking a government to stop doing something, such as returning people to nations where they are suspected of facing death or torture.[36]

[31] (*Omct.org*, 2022) <https://www.omct.org/files/2006/11/3633/handbook1_eng_08_part8.pdf> accessed 21 March 2022.
[32] 'Rules Of Court Rule 62§2' (*Echr.coe.int*, 2019) <https://www.echr.coe.int/Documents/Rules_Court_ENG.pdf> accessed 22 March 2022

[33] Karsai Dániel, 'The Friendly Settlement Procedure And The ECHR | Karsai Dániel Ügyvédi Iroda' (*Karsai Dániel ügyvédi iroda*, 2022) <https://drkarsai.hu/en/friendly-settlement-procedure/> accessed 22 March 2022.
[34] *(Ijrcenter.org*, 2022) <https://ijrcenter.org/european-court-of-human-rights/> accessed 22 March 2022.
[35] 'Factsheet – Interim Measures' (*Echr.coe.int*, 2022) <https://www.echr.coe.int/documents/fs_interim_measures_eng.pdf> accessed 22 March 2022.
[36] 'Interim Measures' (*Echr.coe.int*, 2022) <https://www.echr.coe.int/Documents/Interim_Measures_ENG.pdf> accessed 22 March 2022.

According to Rule 39 of the Rules of Court, the European Court of Human Rights may apply interim measures to any state party to the European Convention on Human Rights.[37] This issue is defined as follows: *'The Chamber or, where appropriate, the President of the Section or a duty judge appointed pursuant to paragraph 4 of this Rule may, at the request of a party or of any other person concerned, or of their own motion, indicate to the parties any interim measure which they considers should be adopted in the interests of the parties or of the proper conduct of the proceedings.'*

During the decision of the Court to adopt interim measures, each request is examined individually and in order of priority. The defendant gets informed after a decision is made to enforce an interim measure. Applicants and governments would be notified of the decisions of the Court on these measures in accordance with Article 39 of the Convention. In some situations, the applicant parties may request the Court to apply interim measures, and these demands may be denied, but there is no way to appeal this decision.[38]

The length of an interim measure is normally determined to cover the duration of the proceedings before the Court or for a shorter period when it is decided to apply. Furthermore, the Court has the power to terminate the implementation of Rule 39 of the Rules of Court at any time. Since these measures are related to the proceedings of the Court, they may be removed if the application is not maintained.[39]

Interim measures, which are only used in a few situations, are usually related to deportation and extradition. It typically involves suspending the deportation or extradition of the applicant while the application is being examined. [40]

The most common situations are those involving fears of:

- a threat to life (situations covered by Article 2 of the Convention)
- ill-treatment prohibited by Article 3 of the Convention (prohibition of torture and cruel or degrading treatment) [41]

[37]'Factsheet – Interim Measures' (*Echr.coe.int*, 2022) <https://www.echr.coe.int/documents/fs_interim_measures_eng.pdf> accessed 22 March 2022.
[38] ibid.
[39] ibid.
[40]'Factsheet – Interim Measures' (*Echr.coe.int*, 2022) <https://www.echr.coe.int/documents/fs_interim_measures_eng.pdf> accessed 23 March 2022.
[41] 'Practice Direction: Requests Of Interim Measures (Rule 39 Of The Rules Of Court)' (*Echr.coe.int*, 2022) <https://www.echr.coe.int/Documents/PD_interim_measures_intro_ENG.pdf> accessed 24 March 2022.

In exceptional circumstances they can also be used to address demands related to the right to respect for private and family life (Article 8 of the Convention) or the right to a fair trial (Article 6 of the Convention).[42]

4. Decision and Judgment

Considering the difference between a decision and a judgment, a decision is usually given by a single judge, a Committee, or a Chamber of the Court and it only concerns the admissibility stage of the case. However, when the admissibility and merits of an application are examined at the same time, as in the process of the Chamber, it will then become a judgment.[43]

Judges may express their 'opposition views,' which include their reasons for disagreement, if they disagree with the majority opinion at the decision stage. They can also write a 'consensus view' if they agree with the majority but want to express their reasons, and these opinions can be found at the end of the judgment.[44]

5. Effects on its Judgments and Enforcement

When the Court issues a judgment finding a violation, it sends the file to the Committee of Ministers of the Council of Europe, which advises the state concerned and the department in charge of enforcing judgments to determine how the judgment should be carried out and how to prevent future violations of the Convention. This can be achieved by a combination of general measures, such as legislative reforms, as well as individual measures, if necessary. Besides that, after a violation has been found, the state concerned must ensure that similar violations do not occur again, otherwise the court may order new judgments against them.[45]

6. Jurisdiction

Individuals and nations may file complaints with the Court alleging violations of the European Convention on Human Rights, which primarily concerns civil and political rights.

[42] 'Factsheet – Interim Measures' (*Echr.coe.int*, 2022) <https://www.echr.coe.int/documents/fs_interim_measures_eng.pdf> accessed 24 March 2022.
[43] (*Echr.coe.int*, 2022) <https://www.echr.coe.int/Documents/50Questions_ENG.pdf> accessed 14 March 2022.
[44] (*Rechtspraak.nl*, 2022) <https://www.rechtspraak.nl/SiteCollectionDocuments/European-court-of-human-rights.pdf> accessed 15 March 2022.
[45] (*Echr.coe.int*, 2022) <https://www.echr.coe.int/Documents/50Questions_ENG.pdf> accessed 14 March 2022.

Article 32 of the current redaction of the Convention defines the jurisdiction of the Court. According to Article 32(1) of the Convention, *'The jurisdiction of the Court shall extend to all matters concerning the interpretation and application of the Convention and the Protocols thereto which are referred to it as provided in Articles 33 (inter-state applications), 34 (individual applications), 46 (referrals by the Committee of Ministers of the Council of Europe of problems of interpretation and execution) and 47 (requests by the Committee of Ministers for advisory opinions).'*[46]

The complaints need to be about alleged violations of the Convention committed by a State Party to the Convention that have a direct and significant impact on the applicant. As of November 2018, the Convention had 47 signatories, including member states of the Council of Europe and the European Union. Some of these countries have also ratified one or more of the Further Protocols of the Convention, which provide additional protection.[47]

On August 1, 2018, the European Court of Human Rights granted advisory jurisdiction under Protocol 16 to the European Convention on Human Rights. Protocol No. 16 broadens the jurisdiction of the Court, and allows the Court to issue advisory opinions on questions of principle relating to the interpretation or application of the rights and freedoms defined in the Convention or its protocols. As a result, it is possible to improve the interaction between the Court and state authorities, thus strengthening the implementation of the Convention in accordance with the subsidiarity concept.[48]

However, it should be noted that the requesting court or tribunal may only seek an advisory opinion in the context of a case that it is already considering. It must provide the Court with the relevant legal and factual background to the pending case, as well as explain the reasons for its request.[49]

[46] Peter Kempees, *"Hard Power" And The European Convention On Human Rights* (Brill 2020). p.225
[47] *(Ijrcenter.org*, 2022) <https://ijrcenter.org/european-court-of-human-rights/> accessed 24 March 2022.

[48] 'What Is A Request For An Advisory Opinion?' (*Echr.coe.int*, 2022) <https://www.echr.coe.int/Documents/Press_Q_A_Advisory_opinion_ENG.PDF> accessed 24 March 2022.
[49] ibid.

II. CASE OF BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM

1. INTRODUCTION TO THE CASE

a. Overview

i. Historical Development of State Surveillance

During the Second World War, the UK and US governments entered into a series of agreements to share signalling intelligence of enemy communications traffic.[50] BRUSA, the 'British-US Communications Intelligence Agreement (1946)', later known as UKUSA, linked the two countries to a worldwide network of interception points managed by the largest intelligence organization of the UK, GCHQ, and its US equivalent, the National Security Agency (NSA).[51] Afterward, ECHELON is the signals intelligence-gathering program run by Allied powers namely 'The Five Eyes' Australia, Canada, New Zealand, the United Kingdom, and the United States, after World War II.[52] This program, based on the UKUSA Agreement, was created in the early 1960s to monitor the military and diplomatic communications of the Soviet Union and Eastern Bloc allies of them during the Cold War.[53]

The European Parliament released a report on ECHELON after a year-long investigation into how the spying system was used to collect sensitive industrial secrets of Europe and pass them on to their British or American rivals, which concluded that a worldwide spy network existed.[54] Nevertheless, ECHELON was largely just another theory of conspiracy, until Snowden made it clear to the full capabilities of the NSA and other government spy agencies.[55]

ii. The Challenges of Protecting Privacy

[50] 'Intelligence Sharing In A Complicated World: The Future Of Five Eyes' (*The Cipher Brief*, 2021) <https://www.thecipherbrief.com/intelligence-sharing-in-a-complicated-world-the-future-of-five-eyes> accessed 13 November 2021.

[51] Richard Norton Taylor, 'Not So Secret: Deal At The Heart Of UK-US Intelligence' (*the Guardian*, 2010) <https://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released> accessed 13 November 2021.

[52] Lucas Matney, 'Techcrunch Is Part Of The Yahoo Family Of Brands' (*Techcrunch.com*, 2015) <https://techcrunch.com/2015/08/03/uncovering-echelon-the-top-secret-nsa-program-that-has-been-watching-you-your-entire-life/> accessed 13 November 2021.

[53] Ibid.

[54] Jane Perrone, 'The Echelon Spy Network' (*the Guardian*, 2001) <https://www.theguardian.com/world/2001/may/29/qanda.janeperrone> accessed 13 November 2021.

[55] Lucas Matney, 'Techcrunch Is Part Of The Yahoo Family Of Brands' (*Techcrunch.com*, 2015) <https://techcrunch.com/2015/08/03/uncovering-echelon-the-top-secret-nsa-program-that-has-been-watching-you-your-entire-life/> accessed 13 November 2021.

Discussions about the legitimate balance between security and information privacy have been going on for several years, especially in areas related to electronic or digital communication between countries.[56]

Transformation of information into digital form, arbitrary data transfer paths, and the location of information in transport and storage are often unpredictable or unknown. This led to the inadequacy of legal regulations.[57] Whether the Internet will continue to be an infrastructure for unlimited communication and access to information, whether it will support freedom of expression, or whether it can be transformed into a control and surveillance tool depends largely on respecting privacy.[58] A comprehensive interpretation of the situation is basically how the balance is established. The goal of balancing any benefit from designing and implementing innovative surveillance capabilities with the value of privacy rights implies the goal of finding a win-win solution.[59] If appropriate decisions are to be made on the enforcement of surveillance and the laws governing surveillance, the surveillance framework should be reshaped by taking necessary and adequate protection measures and maintaining a dual balance without breaking the limits of privacy rights.[60]

The right to privacy is a recent invention as a legal concept and is based on a legal review article published by Samuel Warren and Louis Brandeis[61] in December 1890.[62] Warren and Brandeis noted that it is necessary for the legal system to recognize the right to privacy by reason of when information of the private life of the person is publicized to third parties, there is a tendency to affect or even undermine the core of personality of an individual.[63] This article has created a general infrastructure to revive the right to privacy to the agenda and sheds light on the regulations that have come to the present. General development regarding the right to

[56] Alan F. Westin, 'Science, Privacy, And Freedom: Issues And Proposals For The 1970'S. Part I--The Current Impact Of Surveillance On Privacy' (1966) 66 Columbia Law Review.
[57] Stephen J. Schulhofer, 'An International Right To Privacy? Be Careful What You Wish For' (2016) 14 International Journal of Constitutional Law.
[58] Kevin Walby, 'Review Of Friedewald, Michael, J. Peter Burgess, Johann Čas, Rocco Bellanova, And Walter Peissl. (Eds). Surveillance, Privacy, And Security: Citizens' Perspectives' (2018) 31 Security Journal.
[59] Daniel J. Power, Ciara Heavin and Yvonne O'Connor, 'Balancing Privacy Rights And Surveillance Analytics: A Decision Process Guide' (2021) 4 Journal of Business Analytics.
[60]Paul Bernal, 'Data Gathering, Surveillance And Human Rights: Recasting The Debate' (2016) 1 Journal of Cyber Policy
[61] Samuel D. Warren and Louis D. Brandeis, 'Warren, Samuel & Louis Brandeis. The Right To Privacy, 4 Harv. L. Rev. 193 (1890)' (1890) 25 Communication Law and Policy.
[62] Dorothy J Glancy, 'Invention of the Right to Privacy, The ' (1979) 21 Ariz L Rev 1
[63] Ibid.

privacy, particularly is *Article 12 of the UN Declaration of Human Rights*[64], proclaimed by the United Nations General Assembly on 10 December 1948, includes the right to privacy.[65]

Alan Weston, the author of 'Privacy and Freedom' in 1967, helped lay the cornerstone for modern debates about technology, privacy, and personal freedom. In 'Privacy and Freedom' Weston defined privacy as '*the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*.' Westin stated that citizens should have complete control over their personal data, including how much and to whom it should be disclosed, how it should be stored, and how it should be distributed, providing the framework for current understandings of online privacy laws.[66]

European data protection law builds on the works of the 'Non-Binding Guidelines for the Protection of Privacy and Transborder Flows of Personal Data' of the OECD, and '1981 Convention of the Council of Europe for the Protection of Individuals with Relating to Automatic Processing of Personal Data'.[67] In light of new enhancements, the Data Protection Directive (95/46/EC), adopted in October 1995, aimed to both harmonize the protection of the fundamental rights and freedoms of European citizens regarding their processing activities, and to ensure the flow of personal data between the Member States[68].

In 2012, the European Commission published a draft European Data Protection Regulation to replace the EU Data Protection Directive. Also referred to as the right to be forgotten, the law allows EU citizens to request search engines to have their personal information removed from search results. [69] Lastly, The General Data Protection Regulation (GDPR) became binding law in European Union Member States in 2018 as a step towards harmonization of personal data protection legislation in the European Union. [70] The right to respect for private and family life has been shaped, grown, taken its present form over time as

[64] 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'
[65] 'History Of Privacy Timeline / Safecomputing.Umich.Edu' (*Safecomputing.umich.edu*) <https://safecomputing.umich.edu/privacy/history-of-privacy-timeline> accessed 15 November 2021.
[66] Luisa Rollenhagen, 'Alan Westin Is The Father Of Modern Data Privacy Law | Osano' (*Osano*, 2020) <https://www.osano.com/articles/alan-westin> accessed 15 November 2021.
[67] Edward Dove, 'The EU General Data Protection Regulation: Implications For International Scientific Research In The Digital Era' [2018] SSRN Electronic Journal.
[68] Ibid.
[69] 'History Of Privacy Timeline / Safecomputing.Umich.Edu' (*Safecomputing.umich.edu*) <https://safecomputing.umich.edu/privacy/history-of-privacy-timeline> accessed 15 November 2021.
[70] Antonia Vlahou, 'Data Sharing Under The General Data Protection Regulation' (*Hypertension*, 2021) <https://www.ahajournals.org/doi/10.1161/HYPERTENSIONAHA.120.16340> accessed 15 November 2021.

a result of new privacy systems and advancements, and will continue to be open to new regulations.[71]

iii. Conflicted Concepts: The Right to Privacy versus National Security Interests

Privacy is not a static object that can be captured and defined. It is always related to context, making it impossible to define it without reference to a complex social, cultural, religious, and historical parameter from which it derives its meaning.[72] Private life is often disrupted by outside influences. The right to privacy provides a means of protection against unwanted intrusions. Individual burdens should be kept to a minimum when legitimate disturbances arise.[73]

The notion of national security is a subject that should require comprehensive understanding to strike a balance to the conflicting rights of privacy and security. The concept of 'national security' like 'privacy', is amorphous and devoid of definite meaning. The scope of national security is not limited to situations where the state defends itself against an internal unlawful force threat against its institutions or persons within its borders, it has a wide execution area in terms of international law as well.[74] National security is an easily justified public resource, and there is no more important common national purpose than protecting national security, protecting the lives of citizens, and maintaining public order.[75] Security is a fundamental condition for achieving these goals, without which no consideration can be attached to human rights and other individual and collective interests. As a result, since the concepts of national security and privacy are not fully defined, considering the essence of the conflicted rights to minimize possible violations of rights will be essential for understanding the conflict in question. [76]

The right to respect for private life is a universal international human right.[77] While privacy is normally expressed as a human right, as explained above, perceptions of the right to

[71] Antonia Vlahou, 'Data Sharing Under The General Data Protection Regulation' (*Hypertension*, 2021) <https://www.ahajournals.org/doi/10.1161/HYPERTENSIONAHA.120.16340> accessed 15 November 2021.
[72] Bart Willem Schermer, *Software Agents, Surveillance, And The Right To Privacy: A Legislative Framework For Agent-Enabled Surveillance (SIKS Dissertation Series, 1873-0760 ; No. 2007-05)* (Amsterdam University Press 2007).b
[73] Ibid.
[74] Emanuel Gross, 'The Struggle of a Democracy against Terrorism - Protection of Human Rights: The Right to Privacy versus the National Interest - the Proper Balance' (2004) 37 Cornell Int'l LJ 27
[75] Ibid
[76] Ibid.
[77] Zygmunt Bauman and others, 'After Snowden: Rethinking The Impact Of Surveillance' (2014) 8 International Political Sociology

privacy and violation of privacy can be very subjective and inseparable from broader attitudes.[78] The European Convention on Human Rights (ECHR) sets out a minimum declaration of rights to be protected in each signatory state. It provides a mechanism that allows individuals to enforce it against the State where the State has violated their rights under the Convention and domestic law has failed.[79] The right most openly threatened is the right to respect for private life guaranteed in Article 8.[80] Article 8 of ECHR states;

> *'8(1). Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *8(2). There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'*[81]

While the first paragraph specifies the rights that should be guaranteed to the individual by the state, the second part states under which conditions an interference with these rights may be legitimate.[82] European Convention case-law has interpreted Article 8(2) to mean that no right guaranteed by the Convention should be interfered with for any reason, unless a citizen perceives the basis for the interference through an identifiable national law.[83] Any interference with individual privacy must be subject to the consent of the person, the use of personal information being subject to the consent of the owner, not the consent of the State in question, pursuant to Article 8 of the ECHR.[84] Further consent is only valid if the person knows exactly what they are consenting to directly meets article 8 paragraph (2).

The ECHR has developed some general principles that must be fulfilled by law providing for mass surveillance of communications by public authorities. First, the law must be accessible, and the person concerned must be able to foresee the consequences of the law on his/her own.[85] Intervention must be legally permissible, as well as sufficiently clear and publicly available in order to be predictable. Thus, the behaviour of the person concerned can

[78] Colin J Bennett, 'In Defense Of Privacy: The Concept And The Regime' (2011) 8 Surveillance & Society
[79] Nick Taylor, 'State Surveillance And The Right To Privacy.' (2002) 1 Surveillance & Society.
[80] Ibid.
[81] European Convention on Human Rights (ECHR) art 8
[82] Rikke Frank Joergensen, 'Can Human Rights Law Bend Mass Surveillance?' (2014) 3 Internet Policy Review.
[83] Nick Taylor, 'State Surveillance And The Right To Privacy.' (2002) 1 Surveillance & Society.
[84] Zygmunt Bauman and others, 'After Snowden: Rethinking The Impact Of Surveillance' (2014) 8 International Political Sociology
[85] Ibid.

be adjusted properly. [86]. Second, there should be minimal safeguards for public authorities to exercise their discretion. For instance, there should be detailed rules in domestic law regarding the nature of offenses that could give rise to an interception order.[87] Any exception to a human right permitted by law should be interpreted narrowly, government interference must have a judicial review and anyone who is harmed by the interference should be able to seek justice.[88] Third, adequate and effective safeguards should be taken against abuse, i.e. inspection and examination by the competent authorities.[89] This aspect of the right requires a limitation of purpose for the collection and use of personal data. It prohibits the change of function in cases when the state tries to interfere with the right to collect and use personal data, resulting in a violation of the data privacy subject. This intervention must be justified by state authorities.[90]

States do try to act on a larger area, insisting on privacy impact assessments, advising about new legislative and regulatory measures, auditing information systems, educating citizens as to their rights and responsibilities. However, effectiveness in these roles is limited and variable.[91] Limitations and variability are not able to remove the liability of States. They have an obligation to ensure that private sector actors do not violate the privacy of individuals. They are obliged to regulate the storage and use of personal data by the private sector. The main point to remember is that everyone has the right to respect the privacy of their own life, and therefore personal data must be comprehensively protected. [92]

iv. Mass Surveillance and Communication Data

The digital age has brought about a fundamental shift in government surveillance, both in terms of how it is carried out and what it tries to achieve. This transformation is indicative of communication data techniques that involve large-scale collection, storage and analysis of communication data.[93]

[86] Zygmunt Bauman and others, 'After Snowden: Rethinking The Impact Of Surveillance' (2014) 8 International Political Sociology
[87] Rikke Frank Joergensen, 'Can Human Rights Law Bend Mass Surveillance?' (2014) 3 Internet Policy Review
[88] Zygmunt Bauman and others, 'After Snowden: Rethinking The Impact Of Surveillance' (2014) 8 International Political Sociology
[89] Rikke Frank Joergensen, 'Can Human Rights Law Bend Mass Surveillance?' (2014) 3 Internet Policy Review.
[90] Zygmunt Bauman and others, 'After Snowden: Rethinking The Impact Of Surveillance' (2014) 8 International Political Sociology
[91] Colin J Bennett, 'In Defense Of Privacy: The Concept And The Regime' (2011) 8 Surveillance & Society
[92] Zygmunt Bauman and others, 'After Snowden: Rethinking The Impact Of Surveillance' (2014) 8 International Political Sociology
[93] Murray D and Fussey P, “Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data” (2019) 52 Israel Law Review 31

Image: The impact of technology on the rule of law.[94]

The intelligence and security services of the United Kingdom (UK) report that the use of mass communication data is 'essential' as a key tool in meeting their liabilities to protect human rights. However, in other respect, they have expressed some concerns that serious human rights could be subject to potential violations, especially regarding rights in particular; the right to privacy, the right to freedom of expression, the right to freedom of assembly and association, and the prohibition of discrimination.[95]

i) Understanding Metadata

The terms metadata have been adopted by the computer science, statistics, database, and library and information science communities to mean ‘data about data.’ The term refers to data attributes that describe, provide context, indicate quality, or document other objects (or data) properties.[96] In other words, 'communication data' (or metadata) refers to all communication-related information, except the actual essence of the communication.[97] Metadata is effortless to analyse and collect, formats are standardized, and most are numeric. It is especially important in 'big data'. Content may be written implicitly, by implication, or in a language that is not automatically understood. The idea of truly ‘reading’ or ‘listening to’ content at the scales

[94] Paul Rosenzweig, 'Surveillance Technology And The Rule Of Law' (*The Great Courses Daily*, 2021) <https://www.thegreatcoursesdaily.com/surveillance-technology-and-the-rule-of-law/> accessed 20 March 2022.
[95] Ibid.
[96] Jane Greenberg, 'Understanding Metadata And Metadata Schemes' (2005) 40 Cataloging & Classification Quarterly.
[97] Daragh Murray and Pete Fussey, 'Bulk Surveillance In The Digital Age: Rethinking The Human Rights Law Approach To Bulk Monitoring Of Communications Data' (2019) 52 Israel Law Review.

intended by mass surveillance is impracticable until the very final stages of analysis.[98] Communication data is considered particularly useful for intelligence and security services when collected to create a comprehensive communication record of individual and internet-based activities. Such data is used to find communication patterns or features that may indicate involvement in national threats.[99]

ii) Bulk – Targeted Interceptions

There are two broad types of surveillance capabilities classified as Targeted Intercept and Bulk (Mass) Intercept.[100] The concept of bulk data has been defined as the authoritative collection of large amounts of signal intelligence data obtained.[101] Interception of bulk data can be referred to as undirected or passive surveillance which enables the collection of large volumes of information for future reference. Targeted interception or targeted surveillance focuses on individuals or a Subject of Interest under governmental or judicial oversight. Targeted interception is often reserved for combating serious and organized crime, including terrorism and significant threats to life.[102] In general, targeted interception is used when the focus of the search is known, while bulk interception is used when the target is unknown.[103]

In the United Kingdom bulk interception system, only security and intelligence agencies can apply for a bulk interception warrant and for only three legal purposes: national security, prevention and detection of serious crimes, and to protect the economic well-being of the United Kingdom regarding national security.[104] A bulk interception warrant must set out specific purposes that must be met before the collected data can be examined, i.e., viewed, read or listened to. These specific purposes are approved by a Secretary of State and Judicial Commissioners.[105]

[98] Paul Bernal, 'Data Gathering, Surveillance And Human Rights: Recasting The Debate' (2016) 1 Journal of Cyber Policy.
[99] Daragh Murray and Pete Fussey, 'Bulk Surveillance In The Digital Age: Rethinking The Human Rights Law Approach To Bulk Monitoring Of Communications Data' (2019) 52 Israel Law Review.
[100] David Anstiss, 'What Is Target Intercept Vs Bulk Intercept? - SS8' (*SS8*, 2020) <https://www.ss8.com/what-is-target-intercept-vs-bulk-intercept> accessed 9 March 2022.
[101] Marcello Malagutti, "'Bulk Data: Intelligence And Surveillance.'" [2018] Academia.
[102] David Anstiss, 'What Is Target Intercept Vs Bulk Intercept? - SS8' (*SS8*, 2020) <https://www.ss8.com/what-is-target-intercept-vs-bulk-intercept/> accessed 1 December 2021.
[103] 'Interception, Investigatory Powers Act Factsheet' <https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/03/Interception.pdf> accessed 27 March 2022.
[104] (*Assets.publishing.service.gov.uk*) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473751/Factsheet-Bulk_Interception.pdf> accessed 1 December 2021.
[105] Ibid.

iii) United States Metadata Collection

In June 2013, former National Security Agency employee Edward Snowden disclosed that the US government had engaged in large-scale data collection from both US and foreign citizens through various agencies of the US government. The issue of privacy, surveillance, and mass data collection was brought to the forefront with the disclosure.[106] Data collection was mainly run through two programs namely PRISM and UPSTREAM. The US government confirmed the existence of such programs but claimed that it only targets non-US citizens and is authorized under Foreign Intelligence Surveillance Act (FISA).[107]

Both programs are designed around the fact that different legal frameworks apply to the surveillance of 'foreign' and 'domestic' persons in the US. However, the legal restrictions on surveillance without a warrant do not apply to non-US residents.[108] In principle, there are two distinct surveillance frameworks, but global communication networks as well as the global internet and communication industries appear to have blurred these boundaries.[109]

v. United Kingdom Intelligence Oversight

The surveillance system of the security and intelligence agencies in the UK laid its first foundations when it was revealed that the system by which ministers allowed interception of communications was found to violate the European Convention on Human Rights (*Malone v United Kingdom* [1984]). Then the system was built piecemeal until today. The Regulation of Investigatory Powers Act 2000 (RIPA) helped to rationalize issues to some level.[110] The Investigative Powers Act 2016 (IPA 2016) provides the primary legal framework that governs the use of surveillance by public agencies. This framework was predominantly ruled by the Regulatory Investigative Powers Act 2000.[111] The provisions of RIPA 2000 on the capture and

[106] Glenn Greenwald, *No Place To Hide* (Hamish Hamilton, an imprint of Penguin Books 2015
[107] 'Clapper Admits Secret NSA Surveillance Program To Access User Data' (*the Guardian*, 2021) <https://www.theguardian.com/world/2013/jun/07/clapper-secret-nsa-surveillance-prism> accessed 7 November 2021.
[108] Melissa de Zwart and Sal Humphreys and Beatrix Van Dissel, 'Surveillance, Big Data and Democracy: Lessons for Australia from the US and UK' (2014) 37 UNSWLJ 713
[109] Ibid.
[110] GILL PETER, "The Intelligence and Security Committee and the Challenge of Security Networks" (2009) 35 Review of International Studies 929
[111] 'Regulation Of Investigatory Powers Under RIPA 2000 | Legal Guidance | Lexisnexis' (*Lexisnexis.co.uk*) <https://www.lexisnexis.co.uk/legal/guidance/regulation-of-investigatory-powers-interception-of-communications-under-ripa-2000> accessed 10 November 2021.

acquisition of communication data have been repealed and replaced by IPA 2016.[112] RIPA 2000 is up to date with all changes known to be in force on and will continue in force until expressly repealed. Henceforth RIPA 2000 will be examined from the standpoint of applicable law.

RIPA permits interception of internal and external communications after the issuance of a relevant warrant with different provisions for interception of communications.[113] Warrants for communications transmitted and received within the UK (internal communications) are arranged by section 8(1) of RIPA and warrants for communications between the UK and abroad (external communications) are arranged by section 8(4) of RIPA.[114]

In October 2000, the Investigatory Powers Tribunal was created by RIPA and is the only court allowed to hear complaints against UK intelligence agencies.[115] It can hold public or private hearings and take evidence that is inadmissible in court. If a complaint is upheld, IPT has the power to provide compensation, to reverse or cancel warrants and to request destruction of incorrectly obtained information. In general, IPT may not disclose any information without the consent of the originator.[116]

Between June and December 2013, Ten Human Rights Organisations[117] filed separate applications at the UK Investigatory Powers Tribunal (UK IPT or Tribunal), where their cases were later joined.[118] The main arguments put forward by the applicants were that the UK legal framework regulating the interception of communications and the receipt of communications data and foreign intercept materials were not 'lawful' and therefore constituted an interference with the right to privacy and freedom of expression.[119]

The UK IP Tribunal published rulings on the cases, the UK IPT made extensive reference to the case-law of the ECHR to conclude on the case and recognized that Prism-related activities included the rights to privacy and freedom of expression regulated in articles 8 and 10, respectively. The decision outlined two conditions for interference with Article 8 of the ECHR

[112] Ibid.
[113] Bart van der Sloot & Eleni Kosta, 'Big Brother Watch and Others v UK: Lessons from the Latest Strasbourg Ruling on Bulk Surveillance' (2019) 5 Eur Data Prot L Rev 252
[114] Ibid.
[115] Rubin S Waranch, 'Digital Rights Ireland Deja Vu: Why the Bulk Acquisition Warrant Provisions of the Investigatory Powers Act 2016 Are Incompatible with the Charter of Fundamental Rights of the European Union' (2017) 50 Geo Wash Int'l L Rev 209
[116] GILL PETER, “The Intelligence and Security Committee and the Challenge of Security Networks” (2009) 35 Review of International Studies 929
[117] Amnesty International Limited (Amnesty International), Bytes for All (B4A), The National Council for Civil Liberties (Liberty), Privacy International, The American Civil Liberties Union (ACLU), The Canadian Civil Liberties Association (CCLA), The Egyptian Initiative for Personal Rights (EIPR), The Hungarian Civil Liberties Union (HCLU), The Irish Council for Civil Liberties (ICCL) and The Legal Resources Centre (LRC)
[118] B. van der Sloot and E. Kosta, 'Big Brother Watch And Others V UK: Lessons From The Latest Strasbourg Ruling On Bulk Surveillance' (2019) 5 European Data Protection Law Review.
[119] Ibid.

to be 'lawful'. First, it required there had to be no unlimited discretion for executive action and controls over the arbitrariness of that action. According to the second requirement, the nature of the rules must be clear, and the scope should be as public as possible thus the existence of interference with private life can be foreseeable.[120]

i) Bulk Interception System of the UK

Bulk interception is an entity that allows security and intelligence agencies to intercept communications from individuals inside and outside the UK. It analyses the material to classify communications of intelligence value, obtain and then filter internally and externally focused intelligence, and identify individuals, groups, and organizations overseas who pose a threat to the UK.[121] The data collected or stored can only be accessed by the Security and Intelligence Agencies [SIA]: namely the Security Service [MI5], the Secret Intelligence Service [MI6] and the Government Communications Headquarters [GCHQ].[122]

Work of GCHQ, including interception, is controlled under the Intelligence Services Act (1994) and the Regulation of Investigatory Powers Act (2000). [123] All interference is authorized by a Secretary of State through warrants issued pursuant to one of these Acts.[124]

TEMPORA is the mass surveillance system allegedly administered by the Government Communications Headquarters (GCHQ).[125] It has most likely provided GCHQ the largest Internet access among the 'Five Eyes' group of countries. [126] GCHQ provides mass interception of internet traffic by tapping into undersea fibre optic cables that land in the UK.[127]

[120] Ibid.
[121] DAVID ANDERSON Q.C., 'REPORT OF THE BULK POWERS REVIEW' (*Assets.publishing.service.gov.uk*, 2016) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF> accessed 9 November 2021.
[122] DAVID ANDERSON Q.C., 'REPORT OF THE BULK POWERS REVIEW' (*Assets.publishing.service.gov.uk*, 2016) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF> accessed 9 November 2021.
[123] Ibid.
[124] Sir David Pepper, 'The Business Of Sigint' (2010) 25 Public Policy and Administration.
[125] Ewen MacAskill and others, 'GCHQ Taps Fibre-Optic Cables For Secret Access To World's Communications' (*the Guardian*, 2013) <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> accessed 9 November 2021.
[126] Ilina Georgieva, 'The Right to Privacy under Fire Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR' (2015) 31 Utrecht J Int'l & Eur L 104
[127] Scarlet Kim and others, 'New U.K. Law Fails European Court Standards On Mass Interception Disclosed By Snowden - Just Security' (*Just Security*, 2018) <https://www.justsecurity.org/60878/u-k-law-fails-european-court-standards-mass-interception-snowden-disclosed/> accessed 9 November 2021.

GCHQ selects bearers to block, then routes a copy of the intercepted internet traffic to carriers with temporary storage areas that are reported to store content for three days and metadata for 30 days. This information is then filtered and searched based on selectors and search criteria.[128]

GCHQ was operating two major processing systems regarding the bulk interception. The first processing system targets a portion of carriers that contain certain identifiers from a list of 'simple selectors' such as a specific email or name related to a known destination. The captured data is then subjected to a 'triage process,' which identifies the communications that are most likely to include high-value intelligence.[129] The second system targets the smaller number of carriers most likely to carry intelligence-related communications. 'Processing rules' are used to obtain data from these carriers and then filtered to extract and index potentially high-value communications. Communications are only read by analysts at the end of these processes.[130]

The Intelligence Security Committee reported (2015) that only a small part of the data collected due to processing systems for mass interception of communication can be read. It was also stated that the information passed through the automatic filter system and the information without intelligence value was automatically discarded without passing the upper filtering.[131]

ii) GCHQ Processing System for the Bulk Interception

Brief Info: Selector is an identifier used in Dialed Number Recognition (such as phone number, IMEI, IMSI) or Digital Network Intelligence (such as email address or instant messaging IDs). Selectors can be divided in Soft and Strong Selectors. Soft Selector is a search terms (like keywords) not being strong selectors (like telephone numbers or e-mail addresses). Strong Selector is a specific identifier like a name, (an e-mail or an IP address, a phone number, an IMEI)[132]

[128] Ibid.
[129] Chinmayi Sharma, 'Summary: Big Brother Watch And Others V. The United Kingdom' (*Lawfare*, 2018) <https://www.lawfareblog.com/summary-big-brother-watch-and-others-v-united-kingdom> accessed 2 December 2021.
[130] Ibid.
[131] Claudia Aradau and Tobias Blanke, 'The (Big) Data-Security Assemblage: Knowledge And Critique' (2015) 2 Big Data & Society.
[132] NSA Glossary, '<Hr Style="Height:1Px;Border-Width:0;Color:Gray;Background-Color:Gray;">NSA Glossary' (*Electrospaces.net*, 2022) <https://www.electrospaces.net/p/glossary.html#:~:text=Strong%20Selector%20%2D%20A%20specific%20identifier,an%20AppProcIP%20or%20an%20AppProcMac%20*> accessed 7 February 2022.

All internet communications are divided into smaller parts known as ‘packets’. Each packet includes a portion of the content of the communication, as well as metadata. [133] The sender and recipient, the location and date of the communication, and the subject line are all elements of metadata.[134] Information is filtered according to selectors. The exact scope of allowed selectors is unknown, though common examples are email addresses and phone numbers.[135]

Agencies perform two types of listening, depending on the information they have and what they are trying to achieve as an investigatory tool and as an intelligence-gathering tool.[136]

Investigatory tool: If there is specific information about a threat – for example, if a specific email address is linked to terrorist activities – then Agencies can intercept communications from that person. This is known as ‘targeted interception’ and must be authorized by a Secretary of State.[137]

Intelligence-gathering tool: Bulk Interception is mainly utilized as a discovery tool, and the capability of the GCHQ has interpreted as an intelligence-gathering tool.[138]

Bulk interception includes three stages of filtering, targeting and selection. The first stage is to choose which communication links to access.[139]

- The resources required to process and select relevant data means that in practice GCHQ only has access to a very small percentage of what it can access.
- The system chooses the bearers that are more likely to carry communications about national security threats.
- The second stage is to select which communications to collect from these very few bearers.
- The first processing system uses ‘specific simple selectors’ to decide which items to collect, these are specific identifiers, relating to a known target.

[133] '- Interception Works' (*Privacy International*, 2022) <https://privacyinternational.org/long-read/827/how-bulk-interception-works> accessed 8 February 2022.
[134] 'What Is Metadata (With Examples) - Data Terminology' (*Dataedo.com*, 2022) <https://dataedo.com/kb/data-glossary/what-is-metadata> accessed 8 February 2022.
[135] 'How Bulk Interception Works' (*Privacy International*, 2022) <https://privacyinternational.org/long-read/827/how-bulk-interception-works> accessed 8 February 2022
[136] 'PRIVACY AND SECURITY INQUIRY: OPENING STATEMENT' (*Isc.independent.gov.uk*, 2015) <https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312-ISC-PS-opening-statementweb.pdf> accessed 8 February 2022.
[137] 'Factsheet – Targeted Interception' (*Assets.publishing.service.gov.uk*) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473739/Factsheet-Targeted_Interception.pdf> accessed 8 February 2022.
[138] 'Investigatory Powers Bill, Factsheet – Bulk Interception' (*Assets.publishing.service.gov.uk*) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473751/Factsheet-Bulk_Interception.pdf> accessed 8 February 2022.
[139] 'PRIVACY AND SECURITY INQUIRY: OPENING STATEMENT' (*Isc.independent.gov.uk*, 2015) <https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312-ISC-PS-opening-statementweb.pdf> accessed 8 February 2022

- Another processing system targets an even smaller subset of the bearers GCHQ accesses. This system applies a set of ‘selection rules’ to filter communication.
- The final stage is to decide which of the collected communications to read.[140]
- For communications collected under the firs processing system examined, GCHQ conducts a ‘triage process’ to determine which of the collected communications has the highest intelligence value and should therefore be read.
- Even if communications are known to be related to a known national security target, GCHQ do not have the capacity to read them all, so they must prioritise. Only a very small part of what is collected is read.[141]

iii) Intelligence Sharing with Foreign Governments

Intelligence sharing across national borders has been declared as one of the most promising forms of networked global governance, in which government agencies have made significant progress in detaining terrorists and other dangerous criminals.[142] Transnational intelligence sharing is putting a strain on one of the most critical liberal rights, the right to privacy. Information sharing magnifies and amplifies the privacy risks associated with the processing of personal data instead of surveillance by single government, but it is undeniable that international intelligence cooperation offers enormous potential in the battle against major crime.[143]

[140] Ibid.
[141] James Vincent, 'UK's Online Spying Habits Are Legal But Require Overhaul, Says Government' (*The Verge*, 2015) <https://www.theverge.com/2015/3/12/8198785/gchq-mass-surveillance-isc-report-2015> accessed 8 February 2022.
[142] Francesca Bignami, 'Towards A Right T Ds A Right To Privacy In T Acy In Transnational Intelligence Networks Ansnational Intelligence Network' (2007) 28 Michigan Journal of International Law <https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1173&context=mjil> accessed 2 February 2022.
[143] Dirk Voorhoof, 'Case Law, Strasbourg: Big Brother Watch V United Kingdom, Bulk Interception Regime Violated Articles 8 And 10 – Dirk Voorhoof' (*Inforrm's Blog*, 2021) <https://inforrm.org/2021/06/09/case-law-strasboug-big-brother-watch-v-united-kingdom-bulk-interception-regime-violated-articles-8-and-10-dirk-voorhoof/> accessed 2 December 2021

The main criterion for the protection of the right to privacy is the provision of nationally recognized safeguards within the framework of mutual intelligence agreements. [144] As previously stated, the UK has entered into intelligence agreements with several countries, the most notable of which is the British-US Communication Intelligence Agreement. It is necessary to determine whether the British-US Communication Intelligence Agreement satisfies the minimum standards before evaluating. The alleged violation of the right to privacy and freedom of expression will only be resolved if it is determined whether the data sharing safeguards are sufficient.[145]

The Interception of Communications Code of Practice (IC Code), Section 12, sets out the conditions under which UK intelligence services may request intelligence from foreign intelligence services and the procedures to be followed.[146] The procedure of the regime for requesting and receiving intelligence outlined in Section 12 of the IC Code should adequately accessible.[147] Since the protection of national security, the prevention of disorder and crime, and the protection of rights and freedoms are considered to be legitimate aims, the intelligence-sharing regime should include sufficient safeguards appropriate with the shared data.[148]

vi. The Scope of Freedom of Expression

Freedom of expression refers to the ability of an individual or group of individuals to freely express their opinions, thoughts, ideas, and emotions on a wide range of topics without fear of government repression.[149] Freedom of expression requires a free, uncensored and unrestricted press that can comment and enlighten the public on public matters without fear of censorship or restriction. [150] It is inseparably linked with democracy and is protected by various national, international, and regional institutions that seek to develop a political system that is considered

[144] Bart van der Sloot & Eleni Kosta, 'Big Brother Watch and Others v UK: Lessons from the Latest Strasbourg Ruling on Bulk Surveillance' (2019) 5 Eur Data Prot L Rev 252

[145] Francesca Bignami, 'Towards A Right T Ds A Right To Privacy In T Acy In Transnational Intelligence Networks Ansnational Intelligence Network' (2007) 28 Michigan Journal of International Law

[146] 'Big Brother Watch V. The United Kingdom - Global Freedom Of Expression' (*Global Freedom of Expression*, 2022) <https://globalfreedomofexpression.columbia.edu/cases/big-brother-watch-v-united-kingdom/> accessed 2 February 2022.

[147] Marko Milanovic and others, 'Ecthr Judgment In Big Brother Watch V. UK' (*Ejiltalk.org*, 2022) <https://www.ejiltalk.org/ecthr-judgment-in-big-brother-watch-v-uk/> accessed 2 February 2022.

[148] Rachel C. Taylor, 'Intelligence-Sharing Agreements & International Data Protection: Avoiding a Global Surveillance State' (2018) 17 Wash U Global Stud L Rev 731

[149] 'WHAT IS FREEDOM OF EXPRESSION?' (*Freedom Forum Institute*) <https://www.freedomforuminstitute.org/about/faq/what-is-freedom-of-expression/> accessed 9 March 2022.

[150] Emily Howie, 'Protecting The Human Right To Freedom Of Expression In International Law' (2017) 20 International Journal of Speech-Language Pathology

the only system capable of providing human rights protection.[151] The right has both a personal and a social component and is considered a cornerstone of any democratic society as well as a fundamental requirement for the full development of the person.[152]

The internet does not only facilitate mass communication, but it also provides fertile ground for widespread surveillance. In the digital era, governments use strategies to monitor large segments of the population across national borders e.g., to counter terrorism or other forms of corruption.[153] Whilst mass surveillance is commonly thought of as a privacy issue, it also raises concerns regarding freedom of speech and expression.[154] Mass surveillance methods may mean an indirect interference with freedom of expression. At the very least, they are likely to deter certain users from fully exercising their right to freedom of expression.[155]

Metadata retention regulations that endanger freedom of expression and freedom of the press can deter people from providing information on matters of public concern. This has recently been questioned as an alarming trend.[156] It is necessary to first understand the term 'chilling effect' to gain a broader understanding. In a legal context, a chilling effect is the prevention or deterrence of legitimate exercises of natural and legal rights by the threat of legal sanction.[157] Legal activities such as the passage of a law, a court ruling, or the threat of legal action can have a chilling effect. For example, any legal action that makes people reluctant to exercise a legitimate right because of its legal consequences achieves this result.[158] The chilling effect is considered to be effective in promoting self-censorship and thus reducing transparency in any public sphere. This situation has huge consequences, particularly for the media and journalists.[159] One of the most important aspects of journalism is the capacity to get information while keeping sources safe and secret.[160] Due to mass surveillance systems, governments are

[151] Guide on Article 10 of the European Convention on Human Rights Freedom of Expression (EUCO)[2021]
[152] Emily Howie, 'Protecting The Human Right To Freedom Of Expression In International Law' (2017) 20 International Journal of Speech-Language Pathology.
[153] Maya Hertig Randall, 'Freedom of Expression in the Internet' (2016) 26 Swiss Rev Int'l & Eur L 235
[154] Michael Zimmer, 'Introduction: The "Privacy" Special Issue Of The Journal Of Intellectual Freedom & Privacy' (2017) 2 Journal of Intellectual Freedom & Privacy.
[155] Maya Hertig Randall, 'Freedom of Expression in the Internet' (2016) 26 Swiss Rev Int'l & Eur L 235
[156] Emily Howie, 'Protecting The Human Right To Freedom Of Expression In International Law' (2017) 20 International Journal of Speech-Language Pathology
[157] 'CHILLING EFFECT | Meaning & Definition For UK English | Lexico.Com' (*Lexico Dictionaries | English*, 2022) <https://www.lexico.com/definition/chilling_effect> accessed 7 February 2022.
[158] Allen Green, 'Banish The Libel Chill | Allen Green' (*the Guardian*, 2009) <https://www.theguardian.com/commentisfree/libertycentral/2009/oct/15/simon-singh-libel-laws-chiropractic> accessed 6 December 2021.
[159] Mona Thowsen and Roy Krøvel, *Making Transparency Possible* (2019).
[160] Emily Howie, 'Protecting The Human Right To Freedom Of Expression In International Law' (2017) 20 International Journal of Speech-Language Pathology

alleged to endanger the privacy of sources of journalists by expanding surveillance of telecommunications metadata of the people.[161]

b. Timeline of the Case

1. Former National Security Agency employee Edward Snowden leaked information in 2013 revealing that the US, UK, and other governments use a variety of techniques to collect, store and share communication data via platforms.
2. PRISM is a program that allowed the US government to obtain intelligence from Internet Service Providers. According to National Security Agency (NSA) documents leaked by Edward Snowden, the Government Communications Headquarters (GCHQ) had access to PRISM and used it to generate intelligence reports. GCHQ acknowledges receiving information from the PRISM program of the US.
3. After the revelation, it turned out that the UK uses a program called TEMPORA to enable GCHQ to access communications in bulk and store the massive amounts of data that pass between the UK and the US.
4. In 2014, a group of civil rights organizations (including Big Brother Watch) filed a complaint at the European Court of Human Rights (ECHR) alleging that the mass surveillance and bulk interception system of the UK violates the right to privacy.
5. In 2014, the Bureau of Investigative Journalism, a UK non-profit media organization, filed a second application against the UK, claiming that the mass surveillance system of the UK violates the right to freedom of expression.
6. Per contra, Ten Human Rights Organizations took a different route, launching a legal process at the national level before turning to the ECHR. They made separate applications to the UK Investigatory Powers Tribunal (UK IPT or Tribunal), where their cases were joined.
7. The ECHR prioritized the case against the UK at the Court, which was filed in 2014, but the case was adjourned until the UK IPT delivered its decision.
8. The UK IP Tribunal issued rulings on cases initiated by the Ten Human Rights Organizations. In its first decision, the UK IPT acknowledged that Prism-related activities violated the rights to privacy and freedom of expression, as protected in Articles 8 and 10 of the Convention, respectively.

[161] Emily Howie, 'Protecting The Human Right To Freedom Of Expression In International Law' (2017) 20 International Journal of Speech-Language Pathology

9. The UK IPT accepted that the nature of the rules and their scope should be as clear as possible for the interference to be lawful so that the existence of interference with private life could be foreseen in general terms. IPT concluded that these conditions had not been met and there had been a violation of Article 8 of the Convention.
10. Afterwards, the UK IPT ruled in favour of two of the human rights organizations but did not confirm whether their communications had been intercepted.
11. The ten human rights organizations that were claimants were dissatisfied with the findings of the Tribunal and filed an application against the UK at the ECHR. They claimed that the legal framework governing the interception of communications was not in accordance with the law, and thus violates Articles 8 and 10 of the Convention.
12. The ECHR merged the application with the one submitted by Big Brother Watch and Others v UK.

c. Claims

i. Claims of Big Brother Watch and Others

1. The Applicants allege that bulk interception was neither necessary nor proportionate under the scope of the Right to Privacy of the Convention, therefore did not fall within a margin of appreciation of the State.
2. The applicants allege that all communications (content and/or related communication data), storage, automated processing and examination interfere with the Right to Privacy.
3. The applicants contended that the section 8(4) regime of RIPA is not lawful, as RIPA is overcomplicated, and the full scope and nature of surveillance were only revealed after the 'Snowden Disclosures'.
4. The Applicants allege that the selection of selectors and the selection of material seized for analysis do not have the updated and expanded safeguards. They also claim that the system works without any evidence of doubt regarding any selector or search phrase.
5. The Applicants complain that the distinction between internal and external communications was not only ill-defined but also meaningless, that the vast majority of communications fall under the 'external' category.
6. The applicants allege that the bulk interception system violated the Right to Freedom of Expression, as the large-scale interception and the maintenance of large information databases had a chilling effect on the freedom of expression of journalists.

7. The applicants complain that material seized by the UK authorities under PRISM and Upstream, as well as material received from foreign intelligence services by the NSA, violated the Rights to Privacy.

ii. Claims of The United Kingdom

1. The Government argues that the intelligence gathered under the bulk interception regime was critical to the protection of the United Kingdom from threats to national security.
2. According to the Government, since the path by which electronic communications were transmitted was unpredictable, it was necessary to intercept all communications to obtain even a small fraction of the communications of overseas targets.
3. The Government argues that States should be given a wide margin of appreciation in determining what systems are necessary to protect society from such threats.
4. The Government claims that only if particular communications of a person were selected or examined by an analyst would constitute an infringement on the Right to Privacy. Therefore, the bulk interception system cannot violate the right to privacy due to its nature.
5. The Government claims that no communication or communication data can be viewed by an analyst until it is selected for examination following the automatic filtering process, and no intelligence report can be generated from any communications or related communications data unless viewed by an analyst, therefore there is no violation of the Right to Privacy.
6. The state claims that the aim of the bulk interception regime was not to identify journalistic sources or to target journalists. Therefore, the interference with freedom of expression as a result of the measures of the regime will not be considered 'particularly serious' and there is no violation of the Right to Freedom of Expression.
7. The Government argues that there was no basis to believe the applicants were at risk of their communications being intercepted under PRISM or Upstream or requested by the UK intelligence services. The applicants were unlikely to be affected by legislation allowing for intelligence sharing.

d. Established Agenda of the Court

1. The Bulk Interception of Communication;
    a. Does the section 8(4) regime include the following safeguards:
        i. the nature of offences which may give rise to an interception order,

ii. a definition of the categories of people liable to have their communications intercepted,

b. The scope of the upper safeguards should be considered with the following safeguards :

i. whether the grounds on which a warrant can be issued are sufficiently clear,

ii. whether domestic law provides citizens with an adequate indication of the conditions under which their communications may be intercepted,

iii. whether domestic law provides citizens with an adequate indication of the conditions under which their communications can be selected for review,

2. Intelligence Sharing with Foreign Governments;

a. Does the regime that regulates the receipt of intercept material from foreign intelligence services have the following safeguards:

i. the circumstances in which interception may be requested so limited that States cannot exercise their power to circumvent domestic law or Convention obligations,

ii. a limit on the duration of interception,

iii. the procedure to be followed for examining, using and storing the data obtained,

iv. the precautions to be taken when communicating the data to other parties,

v. the circumstances in which intercepted data may or must be erased or destroyed,

3. Article 10-Right to Freedom of Expression;

a. The Court must consider:

i. whether the interference would be greater if communications were selected for examination,

ii. Whether the conditions under which such communications may be selected for examination are sufficiently clear in domestic law,

iii. whether adequate safeguards are in place to ensure the protection of privacy where such communications are selected for examination.

3. APPLICABLE LAW

a. Conventions

i. The European Convention on Human Rights

i) Article 8- Right to respect for private and family life

> *'1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'*[162]

Article 8(2) means that no right guaranteed by the Convention should be interfered with unless a citizen knows, through an identifiable national law, the basis for the interference, whatever the aim pursued (Malone v UK (1984) 7 EHRR 14, Leander v Sweden (1987) 9 EHRR 433). The law needs to be particularly clear since interception of communications represents a serious interference with private life (Kopp v Switzerland (1999) 27 EHRR 91).[163]

If a primary right is involved in a particular case, any interference with that right must have a legitimate aim. The restrictions that can be justified in terms of the right to private life are regulated in Article 8(2).[164]

ii) Article 10- Right to Freedom of Expression

> *'1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*
> *2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security,*

[162] European Convention On Human Rights (as amended by Protocols Nos. 11, 14 and 15)(ECHR) art 8
[163] Nick Taylor, 'State Surveillance And The Right To Privacy.' (2002) 1 Surveillance & Society.
[164] Ibid.

territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.'[165]

Freedom of expression is a conditional but not absolute right. It is subject to the conditions and limitations stated in article 10(2). It may be subject to legal requirements, conditions, restrictions, or punishments that are necessary in a democratic society.[166]

The notion of 'chilling effect' refers to a negative deterrent to communication. It means deterring a person or organization by indirectly influencing them while exercising their right to freedom of expression. In this context, determining the extent of the 'chilling effect' of the mass surveillance system on the freedom of expression plays an important role.[167]

ii. Universal Declaration of Human Rights

i) Article 12

'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'[168]

ii) Article 19

'Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.'[169]

b. Relevant International Law

i. The United Nations Resolution no. 68/167

'The General Assembly,

[165] European Convention On Human Rights (as amended by Protocols Nos. 11, 14 and 15)(ECHR) art 10
[166] Trine Baumbach, 'Chilling Effect As A European Court Of Human Rights' Concept In Media Law Cases' (2018) 6 Bergen Journal of Criminal Law & Criminal Justice.
[167] Judith Townend, 'Freedom Of Expression And The Chilling Effect' (*Academia.edu*, 2022) <https://www.academia.edu/34350408/Freedom_of_Expression_and_the_Chilling_Effect> accessed 16 February 2022.
[168] Universal Declaration of Human Rights(UDHR) art 12
[169] Universal Declaration of Human Rights(UDHR) art 19

...

4. Calls upon all States:

...

(c) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

(d) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data ...'[170]

ii. The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981

i) Article 1- Object and Purpose

'The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection').'[171]

ii) Article 8 -Additional Safeguards for the Data Subject

'Any person shall be enabled:

a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

[170] UNGA Res 68/167 (18 December 2013) UN Doc A/RES/68/167

[171] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) CETS 108 art 1

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.'[172]

c. EU Law

i. Charter of Fundamental Rights of the European Union

i) Article 7 – Respect for private and family life

'Everyone has the right to respect for his or her private and family life, home and communications.'[173]

ii) Article 8 – Protection of personal data

'1.Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.'[174]

iii) Article 11 – Freedom of expression and information

'1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

2.The freedom and pluralism of the media shall be respected.'[175]

ii. Relevant case-law of the Court of Justice of the European Union

[172] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) CETS 108 art 8
[173] Charter of Fundamental Rights of the European Union (2012) (CFR) C 306/02 art 7
[174] Charter of Fundamental Rights of the European Union (2012) (CFR) C 306/02 art 8
[175] Charter of Fundamental Rights of the European Union (2012) (CFR) C 306/02 art 11

i) Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others (Cases C-293/12 and C-594/12; ECLI:EU:C:2014:238)

'Directive 2006/24 applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives, and covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population.

First, Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime. Secondly, Directive 2006/24 fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Thirdly, Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned. Furthermore, it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary. Consequently, Directive 2006/24 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. Finally, Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data'.[176]

[176] Digital Rights Ireland Ltd V Minister For Communications, Marine And Natural Resources And Others And Kärntner Landesregierung And Others EU:C:2014:238(Summary) [2014] CJEU

ii) Ministerio Fiscal (Case C-207/16; ECLI:EU:C:2018:788)

'Article 15(1) of 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), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that the access of public authorities to data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone, such as the surnames, forenames and, if need be, addresses of the owners, entails interference with their fundamental rights, enshrined in those articles of the Charter of Fundamental Rights, which is not sufficiently serious to entail that access being limited, in the area of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime.'[177]

d. Relevant Domestic Law

i. The Interception of Communication under RIPA

i) Warrants: General

The Regulation of Investigatory Powers Act addresses mass surveillance measures and their review. Section 1 of RIPA 2000 contains the general prohibition to intercept any communication (via e-mails, letters, etc.). The exception is Section 5 of the RIPA, which regulates interception warrants.[178]

The Secretary of State has the authority to order the interception and disclosure of communications in the interests of national security, economic well-being, or the prevention and detection of serious crime. To obtain such a warrant, intelligence agencies must apply to the Secretary of State under Section 6 RIPA. [179]

[177] Case C-207/16 Ministerio Fiscal EU:C:2018:788 [2018] CJEU para 66

[178] 'Regulation Of Investigatory Powers Act 2000/Part I - ORG Wiki' (*Wiki.openrightsgroup.org*) <https://wiki.openrightsgroup.org/wiki/Regulation_of_Investigatory_Powers_Act_2000/Part_I> accessed 6 February 2022.

[179] Felix Bieker, 'Can Courts Provide Effective Remedies Against Violations Of Fundamental Rights By Mass Surveillance? The Case Of The United Kingdom' (2016) 476 Springer <https://doi.org/10.1007/978-3-319-41763-9_20> accessed 1 March 2022.

According to Section 5(2) RIPA the Secretary of State must believe the warrant is necessary and proportionate to achieve the goals set out in Section 5(3) namely*:* [180]

'(3) Subject to the following provisions of this section, a warrant is necessary on grounds falling within this subsection if it is necessary—

(a) in the interests of national security;

(b) for the purpose of preventing or detecting serious crime;

(c) for the purpose of safeguarding the economic well-being of the United Kingdom.' [181]

Section 8 RIPA distinguishes between targeted and bulk warrants. Targeted warrants, as defined by Section 8(1) RIPA, are issued for specified individuals or premises. Bulk warrants address interception of external communications under Sections 8(4) and (5).[182] Section 8 is important in providing 'a description of the seized material that the Secretary of State considers necessary for review'. [183] In general, warrants are required to intercept and examine materials but there are also materials seized without being analysed. These are taken without the need for a warrant by the Secretary of State.[184]

ii) Warrants: Section 8(4) of the RIPA

'(4) Subsections (1) and (2) shall not apply to an interception warrant if:

(a) the description of communications to which the warrant relates confines the conduct authorised or required by the warrant to conduct falling within subsection (5); and

(b) at the time of the issue of the warrant, a certificate applicable to the warrant has been issued by the Secretary of State certifying:

(i) the descriptions of intercepted material the examination of which he considers necessary; and

[180] (*Assets.publishing.service.gov.uk*, 2016) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/496064/53659_CoP_Communications_Accessible.pdf> accessed 6 February 2022.

[181] Regulation of Investigatory Powers Act 2000, s 5(3)

[182] Felix Bieker, 'Can Courts Provide Effective Remedies Against Violations Of Fundamental Rights By Mass Surveillance? The Case Of The United Kingdom' (2016) 476 Springer <https://doi.org/10.1007/978-3-319-41763-9_20> accessed 1 March 2022.

[183] Democratic Audit UK, 'If The Intelligence And Security Committee Is To Be An Effective Scrutineer, It Must Be Able To Rely On The Accuracy Of The Information Provided By The Security Services' (*Democratic Audit*, 2014) <https://www.democraticaudit.com/2014/11/11/if-the-intelligence-and-security-committee-is-to-be-an-effective-scrutineer-it-must-be-able-to-rely-on-the-accuracy-of-the-information-provided-by-the-security-services/> accessed 15 February 2022.

[184] Ibid.

(ii) that he considers the examination of material of those descriptions necessary as mentioned in section 5(3)(a), (b) or (c).'[185]

RIPA Section 8(4) allows for bulk interception of both content and 'related communication data' (essentially metadata). [186] This section refers to the interception of external communications with the permission of the Secretary of State.[187]

'***Section 81*** *(1) In this Act—*

'communication'includes—

(a) (except in the definition of "postal service" in section 2(1)) anything transmitted by means of a postal service;

(b) anything comprising speech, music, sounds, visual images or data of any description; and

(c) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus.'[188]

The term communication is adequately defined in section 81 of the RIPA. The term external communication is defined in Section 20. External communication defines as any communication sent or received outside of the British Island. The Section 8(4) regime does not place any restrictions on the types of external communications in question and as a result, the broad definition of communications in section 81 fully applies.[189]

'Section 8 (5) Conduct falls within this subsection if it consists in;

(a) the interception of external communications in the course of their transmission by means of a telecommunication system;' [190]

In principle, anything that falls under this definition may fall under section 8(5)(a) if it is external.[191]

Sections 8(4) and (5) of the RIPA allow the Secretary of State to issue an order to intercept external communications during transmission through a telecommunications system

[185] Regulation of Investigatory Powers Act 2000, s 8(4).
[186] Julia Hörnle, 'How To Control Interception-Does The UK Strike The Right Balance?' (2010) 26 Computer Law & Security Review.
[187] Maria Tzanou, 'Big Brother Watch And Others V. The United Kingdom: A Victory Of Human Rights Over Modern Digital Surveillance?' (*Verfassungsblog*, 2018) <https://verfassungsblog.de/big-brother-watch-and-others-v-the-united-kingdom-a-victory-of-human-rights-over-modern-digital-surveillance/> accessed 2 March 2022.
[188] Regulation of Investigatory Powers Act 2000, s 81(1).
[189] Lubin A, "Big Brother Watch v. UK (Eur. Ct. H.R. Grand Chamber)" [2022] International Legal Materials 1
[190] Regulation of Investigatory Powers Act 2000, s 8(5)(a).
[191] Lubin A, "Big Brother Watch v. UK (Eur. Ct. H.R. Grand Chamber)" [2022] International Legal Materials 1

.[192] If the criteria in sections 8(4) and (5) are met, in short when the communication is an 'external' communication, that falls within the scope of bulk interception. This allows interception of all communications transmitted via cable or carried by a particular Communication Service Provider (CSP). [193]

The execution of the warrant of the RIPA 8(4) can be identified in four stages:

First, communications from a small percentage of bearers selected as most likely to carry external communications of intelligence value are intercepted, second, intercepted communications that are least likely to have intelligence value will be filtered and automatically discarded, third, to select communications that may have intelligence value, matches and criteria are retained, simple selectors and complex search criteria (possibly involving profiling) are applied to communications that are not discarded. Forth, some (if not all) of the remaining data is reviewed by an analyst.[194]

iii) Section 16 Safeguards

Section 15: General Safeguards

Safeguards ensure that the seized material is only read, viewed, or listened to by anyone to the extent that it is certified. It controls the use of selection factors that refer to communications by individuals currently known to be in the British Islands. The certificate provides that a selection process is applied to material seized under section 8(4) to make only the material described in the certificate suitable for human examination. No other authority is allowed to access the data other than that permitted by the certificate. [195]

All material intercepted under the authority of warrants, sections 8(1) or 8(4) of RIPA, and any related communication data should be handled according to the safeguards approved by the Secretary of State in accordance with the duty imposed by RIPA. Pursuant to Section 15(1), with respect to all interception warrants, it is the duty of the Secretary of State to ensure that such arrangements are in effect as he/she considers necessary. The safeguards must meet

[192] (*Assets.publishing.service.gov.uk*, 2016) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/496064/53659_CoP_Communications_Accessible.pdf> accessed 6 February 2022

[193] Ibid.

[194] Judith Vermeulen, 'Big Brother May Continue Watching You' [2018] Ghent: Human Rights Centre <https://biblio.ugent.be/publication/8612719> accessed 15 February 2022.

[195] (*Assets.publishing.service.gov.uk*, 2016) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/496064/53659_CoP_Communications_Accessible.pdf> accessed 16 February 2022

the requirements of section 15 of RIPA. The safeguards of section 16 of RIPA apply to warrants that comply with section 8(4). [196]

Section 16: Additional Safeguards for Warrant 8(4):

Section 16(1) provided:

> *'For the purposes of section 15 the requirements of this section, in the case of a warrant in relation to which there is a section 8(4) certificate, are that the intercepted material is read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant to the extent only that it—*
> *(a) has been certified as material the examination of which is necessary as mentioned in section 5(3)(a), (b) or (c); and*
> *(b) falls within subsection (2).'*[197]
>
> Section 16(2)provided :
>
> *'Subject to subsections (3) and (4), intercepted material falls within this subsection so far only as it is selected to be read, looked at or listened to otherwise than according to a factor which–*
> *a. is referable to an individual who is known to be for the time being in the British Islands; and*
> *b. has as its purpose, or one of its purposes, the identification of material contained in communications sent by him, or intended for him.'*[198]
>
> Section 16(5) provided:
>
> *'Those conditions are satisfied in relation to the selection of intercepted material if –*
> *(a) it has appeared to the person to whom the warrant is addressed that there has been such a relevant change of circumstances as, but for subsection (4)(b), would prevent the intercepted material from falling within subsection (2);*
> *(b) since it first so appeared, a written authorisation to read, look at or listen to the material has been given by a senior official; and*
> *(c) the selection is made before the end of the permitted period'.*[199]

[196] (*Assets.publishing.service.gov.uk*, 2016) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/496064/53659_CoP_Communications_Accessible.pdf> accessed 6 February 2022

[197] Regulation of Investigatory Powers Act 2000, s 16(1)

[198] Regulation of Investigatory Powers Act 2000, s 16(2)

[199] Regulation of Investigatory Powers Act 2000, s 16(5)

In general, automated systems should be used whenever technically possible to carry out selection pursuant to section 16(1) of RIPA. As an exception, a certificate may allow seized material to be accessed by a limited number of authorized persons without being processed or filtered by automated systems. This access may only be permitted to the extent necessary to determine whether the material falls within the major categories to be selected for certification. Such control should be necessary for the reasons set out in section 5(3) of RIPA. After performing these functions, all copies made materials intended for these purposes must be destroyed in accordance with section 15(3) of RIPA. Such checks by the authorities should be kept to an absolute minimum, where possible, automated selection techniques should be used instead.[200]

Before an authorized person reads, views, or listens to the material, a record must be created stating that access to the material is required and proportionate in accordance with section 16 and applicable certification. Periodic audits should be conducted to ensure that the requirements set out in Part 16 of RIPA are met. These checks are made to ensure that records requesting access to material to be read, viewed or listened to are compiled correctly and that the requested material falls within the subjects approved by the Secretary of State.[201]

ii. Intelligence Sharing

i) The Interception of Communication Code of Practice

> ***'Rules for Requesting and Handling Unanalysed Intercepted Communications Content and Secondary Data from Overseas authorities***
>
> ***Application of this chapter***
>
> *This chapter applies to those intercepting agencies that undertake interception under a section 8(4) warrant.*
>
> ***Requests for assistance other than in accordance with a mutual assistance agreement***
>
> *A request may only be made by an intercepting agency to the government of a country or territory outside the UK for unanalysed intercepted communications (and associated communications data), otherwise than in accordance with an international mutual assistance agreement, if either:*

[200] (*Assets.publishing.service.gov.uk*, 2016) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/496064/536599_CoP_Communications_Accessible.pdf> accessed 6 February 2022.
[201] Ibid.

- *A relevant interception warrant under RIPA has already been issued by the Secretary of State, the assistance of the foreign government is necessary to obtain the particular communications because they cannot be obtained under the relevant RIPA interception warrant and it is necessary and proportionate for the intercepting agency to obtain those communications; or*
- *Making the request for the particular communications in the absence of a relevant RIPA interception warrant does not amount to a deliberate circumvention of RIPA or otherwise frustrate the objectives of RIPA (for example, because it is not technically feasible to obtain the communications via RIPA interception), and it is necessary and proportionate for the intercepting agency to obtain those communications*

  A request falling within the second bullet of paragraph 12.2 may only be made in exceptional circumstances and must be considered and decided upon by the Secretary of State personally.

  For these purposes, a "relevant RIPA interception warrant" means one of the following: (i) a section 8(1) warrant in relation to the subject at issue; (ii) a section 8(4) warrant and an accompanying certificate which includes one or more "descriptions of intercepted material" (within the meaning of section 8(4)(b) of RIPA) covering the subject's communications, together with an appropriate section 16(3) modification (for individuals known to be within the British Islands); or (iii) a section 8(4) warrant and an accompanying certificate which includes one or more "descriptions of intercepted material" covering the subject's communications (for other individuals).

  Safeguards applicable to the handling of unanalysed intercepted communications from an overseas authority

  If a request falling within the second bullet of paragraph 12.2 is approved by the Secretary of State other than in relation to specific selectors, any communications obtained must not be examined by the intercepting agency according to any factors as are mentioned in section 16(2)(a) and (b) of RIPA unless the Secretary of State has personally considered and approved the examination of those communications by reference to such factors.[202]

[202] All other requests within paragraph 12.2 (whether with or without a relevant RIPA interception warrant) will be made for material to, from or about specific selectors (relating therefore to a specific individual or individuals). In these circumstances the Secretary of State will already therefore have approved the request for the specific individual(s) as set out in paragraphs 12.2.

Where intercepted communications content or communications data are obtained by the intercepting agencies as set out in paragraph 12.2, or are otherwise received by them from the government of a country or territory outside the UK in circumstances where the material identifies itself as the product of an interception, (except in accordance with an international mutual assistance agreement), the communications content[203] and communications data[204] must be subject to the same internal rules and safeguards that apply to the same categories of content or data when they are obtained directly by the intercepting agencies as a result of interception under RIPA.

All requests in the absence of a relevant RIPA interception warrant to the government of a country or territory outside the UK for unanalysed intercepted communications (and associated communications data) will be notified to the Interception of Communications Commissioner'.[205]

The transferred bulk material must be shared in accordance with the procedure required at the national level. This must be duly authorized by the intelligence agency.[206]

IV. CONCLUSION

Mass surveillance systems that focus on the detection of criminality in terms of personal data accessible to the State and how and why this data is processed and analysed has been one of the key aspects of the fight against major crimes for States. On the other hand, the right to privacy and the rights to freedom of expression and association may be threatened by the surveillance system, where effective safeguards are not implemented or regularly updated as new needs arise.

In the case of Big Brother Watch v. UK, the Court will examine the legality and limitations of surveillance from the perspective of the Right to Privacy and Right to Freedom

[203] Whether analysed or unanalysed.
[204] Whether or not those data are associated with the content of communications.
[205] 'Interception Of Communications Code Of Practice Pursuant To Section 71 Of The Regulation Of Investigatory Powers Act 2000' (*Assets.publishing.service.gov.uk*, 2016) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/496064/53659_CoP_Communications_Accessible.pdf> accessed 23 February 2022.
[206] Judith Vermeulen, 'Big Brother May Continue Watching You' [2018] Ghent: Human Rights Centre <https://biblio.ugent.be/publication/8612719> accessed 15 February 2022

of Expression under the European Convention on Human Rights. As the concept of mass surveillance is likely to continue and vital for States, important questions of future privacy protection and freedom of expression will be addressed at both national and international levels.

V. BIBLIOGRAPHY

1. (*Assets.publishing.service.gov.uk*, 2022) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473751/Factsheet-Bulk_Interception.pdf> accessed 1 December 2021
2. (Echr.coe.int, 2022)
3. (Echr.coe.int, 2022) <https://www.echr.coe.int/Documents/50Questions_ENG.pdf> accessed 11 March 2022.
4. (Echr.coe.int, 2022) <https://www.echr.coe.int/Documents/50Questions_ENG.pdf> accessed 14 March 2022.
5. (Ijrcenter.org, 2022)
6. (Ijrcenter.org, 2022) <https://ijrcenter.org/european-court-of-human-rights/> accessed 11 March 2022.
7. (Ijrcenter.org, 2022) <https://ijrcenter.org/european-court-of-human-rights/> accessed 16 March 2022.
8. (Ijrcenter.org, 2022) <https://ijrcenter.org/european-court-of-human-rights/> accessed 22 March 2022.
9. (Ijrcenter.org, 2022) <https://ijrcenter.org/european-court-of-human-rights/> accessed 24 March 2022.
10. (Omct.org, 2022) <https://www.omct.org/files/2006/11/3633/handbook1_eng_08_part8.pdf> accessed 21 March 2022.
11. (Rechtspraak.nl, 2022) <https://www.rechtspraak.nl/SiteCollectionDocuments/European-court-of-human-rights.pdf> accessed 13 March 2022.
12. (Rechtspraak.nl, 2022) <https://www.rechtspraak.nl/SiteCollectionDocuments/European-court-of-human-rights.pdf> accessed 13 March 2022.

13. (Rechtspraak.nl, 2022) <https://www.rechtspraak.nl/SiteCollectionDocuments/European-court-of-human-rights.pdf> accessed 13 March 2022.
14. (Rechtspraak.nl, 2022) <https://www.rechtspraak.nl/SiteCollectionDocuments/European-court-of-human-rights.pdf> accessed 15 March 2022.
15. 'Interception Works' (*Privacy International*, 2022) <https://privacyinternational.org/long-read/827/how-bulk-interception-works> accessed 8 February 2022.
    a. <https://ijrcenter.org/european-court-of-human-rights/> accessed 8 March 2022.
    b. <https://www.echr.coe.int/Documents/50Questions_ENG.pdf> accessed 10 March 2022.
16. 'A Brief History Of The European Court Of Human Rights - Eachother' (EachOther, 2022) <https://eachother.org.uk/brief-history-european-court-human-rights/> accessed 10 March 2022.
17. 'A Brief History Of The European Court Of Human Rights - Eachother' (EachOther, 2022) <https://eachother.org.uk/brief-history-european-court-human-rights/> accessed 15 March 2022.
18. 'A Brief History Of The European Court Of Human Rights - Eachother' (EachOther, 2022) <https://eachother.org.uk/brief-history-european-court-human-rights/> accessed 15 March 2022.
19. Amnesty International Limited (Amnesty International), Bytes for All (B4A), The National Council for Civil Liberties (Liberty), Privacy International, The American Civil Liberties Union (ACLU), The Canadian Civil Liberties Association (CCLA), The Egyptian Initiative for Personal Rights (EIPR), The Hungarian Civil Liberties Union (HCLU), The Irish Council for Civil Liberties (ICCL) and The Legal Resources Centre (LRC)
20. Anderson Q.C. D, 'REPORT OF THE BULK POWERS REVIEW' (Assets.publishing.service.gov.uk, 2016) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF> accessed 9 March 2022

21. Anstiss D, 'What Is Target Intercept Vs Bulk Intercept? - SS8' (*SS8*, 2020) <https://www.ss8.com/what-is-target-intercept-vs-bulk-intercept> accessed 9 March 2022.
22. Aradau C and Blanke T, 'The (Big) Data-Security Assemblage: Knowledge And Critique' (2015) 2 Big Data & Society.
23. Bauman Z. and others, 'After Snowden: Rethinking The Impact Of Surveillance' (2014) 8 International Political Sociology
24. Baumbach T, 'Chilling Effect As A European Court Of Human Rights' Concept In Media Law Cases' (2018) 6 Bergen Journal of Criminal Law & Criminal Justice.
25. Bennett C.J., 'In Defense Of Privacy: The Concept And The Regime' (2011) 8 Surveillance & Society
26. Bernal P, 'Data Gathering, Surveillance And Human Rights: Recasting The Debate' (2016) 1 Journal of Cyber Policy.
27. Bernal P, 'Data Gathering, Surveillance And Human Rights: Recasting The Debate' (2016) 1 Journal of Cyber Policy
28. Bieker F, 'Can Courts Provide Effective Remedies Against Violations Of Fundamental Rights By Mass Surveillance? The Case Of The United Kingdom' (2016) 476 Springer <https://doi.org/10.1007/978-3-319-41763-9_20> accessed 1 March 2022.
29. 'Big Brother Watch V. The United Kingdom - Global Freedom Of Expression' (*Global Freedom of Expression*, 2022) <https://globalfreedomofexpression.columbia.edu/cases/big-brother-watch-v-united-kingdom/> accessed 2 February 2022
30. Bignami F, 'Towards A Right T Ds A Right To Privacy In T Acy In Transnational Intelligence Networks Ansnational Intelligence Network' (2007) 28 Michigan Journal of International Law
31. Bignami F, 'Towards A Right T Ds A Right To Privacy In T Acy In Transnational Intelligence Networks Ansnational Intelligence Network' (2007) 28 Michigan Journal of International Law <https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1173&context=mjil> accessed 2 February 2022.
32. Case C-207/16 Ministerio Fiscal EU:C:2018:788 [2018] CJEU para 66
33. Charter of Fundamental Rights of the European Union (2012) (CFR) C 306/02 art 7
34. Charter of Fundamental Rights of the European Union (2012) (CFR) C 306/02 art 8
35. Charter of Fundamental Rights of the European Union (2012) (CFR) C 306/02 art 11

36. 'CHILLING EFFECT | Meaning & Definition For UK English | Lexico.Com' (*Lexico Dictionaries | English*, 2022) <https://www.lexico.com/definition/chilling_effect> accessed 7 February 2022.
37. 'Clapper Admits Secret NSA Surveillance Program To Access User Data' (*the Guardian*, 2021) <https://www.theguardian.com/world/2013/jun/07/clapper-secret-nsa-surveillance-prism> accessed 7 November 2021.
38. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) CETS 108 art 1
39. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) CETS 108 art 8
40. Council of Europe, 'Guide To The Case-Law Of The European Court Of Human Rights-Data Protection' (2021) p.31
41. Democratic Audit UK, 'If The Intelligence And Security Committee Is To Be An Effective Scrutineer, It Must Be Able To Rely On The Accuracy Of The Information Provided By The Security Services' (*Democratic Audit*, 2014) <https://www.democraticaudit.com/2014/11/11/if-the-intelligence-and-security-committee-is-to-be-an-effective-scrutineer-it-must-be-able-to-rely-on-the-accuracy-of-the-information-provided-by-the-security-services/> accessed 15 February 2022.
42. Digital Rights Ireland Ltd V Minister For Communications, Marine And Natural Resources And Others And Kärntner Landesregierung And Others EU:C:2014:238(Summary) [2014] CJEU
43. Dove E, 'The EU General Data Protection Regulation: Implications For International Scientific Research In The Digital Era' [2018] SSRN Electronic Journal.
44. European Convention On Human Rights (as amended by Protocols Nos. 11, 14 and 15)(ECHR) art 8
45. European Convention On Human Rights (as amended by Protocols Nos. 11, 14 and 15)(ECHR) art 10
46. European Convention on Human Rights (ECHR) art 8
47. 'European Convention On Human Rights | Summary, History, & Facts' (Encyclopedia Britannica, 2022) <https://www.britannica.com/event/European-Convention-on-Human-Rights-Europe-1950> accessed 10 March 2022.

48. 'European Court Of Human Rights (Strasbourg,1994)' <https://structurae.net/en/structures/european-court-of-human-rights> accessed 30 March 2022
49. 'European Human Rights System - Research Guides' (Library.law.columbia.edu, 2022) <http://library.law.columbia.edu/guides/European_Human_Rights_System#The_European_Human_Rights_System._The_Commission_of_Human_Rights._How_to_Find_a_Report_of_the_Commission> accessed 20 March 2022.
50. 'Factsheet – Interim Measures' (Echr.coe.int, 2022) <https://www.echr.coe.int/documents/fs_interim_measures_eng.pdf> accessed 22 March 2022.
51. 'Factsheet – Interim Measures' (Echr.coe.int, 2022) <https://www.echr.coe.int/documents/fs_interim_measures_eng.pdf> accessed 22 March 2022.
52. 'Factsheet – Interim Measures' (Echr.coe.int, 2022) <https://www.echr.coe.int/documents/fs_interim_measures_eng.pdf> accessed 23 March 2022.
53. 'Factsheet – Interim Measures' (Echr.coe.int, 2022) <https://www.echr.coe.int/documents/fs_interim_measures_eng.pdf> accessed 24 March 2022.
54. 'Factsheet – Targeted Interception' (*Assets.publishing.service.gov.uk*) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473739/Factsheet-Targeted_Interception.pdf> accessed 8 February 2022.
55. Georgieva I, 'The Right to Privacy under Fire Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR' (2015) 31 Utrecht J Int'l & Eur L 104
56. Glancy D.J., 'Invention of the Right to Privacy, The ' (1979) 21 Ariz L Rev 1
57. Green A, 'Banish The Libel Chill | Allen Green' (*the Guardian*, 2009) <https://www.theguardian.com/commentisfree/libertycentral/2009/oct/15/simon-singh-libel-laws-chiropractic> accessed 6 December 2021
58. Greenberg J, 'Understanding Metadata And Metadata Schemes' (2005) 40 Cataloging & Classification Quarterly
59. Greenwald G, *No Place To Hide* (Hamish Hamilton, an imprint of Penguin Books 2015)

60. Gross E, 'The Struggle of a Democracy against Terrorism - Protection of Human Rights: The Right to Privacy versus the National Interest - the Proper Balance' (2004) 37 Cornell Int'l LJ 27
61. Guide on Article 10 of the European Convention on Human Rights Freedom of Expression (EUCO)[2021]
    A. H. Robertson, 'The European Court of Human Rights' (1960) 9 Am J Comp L 1 p.1
62. Hert P and Malgieri G, 'Article 8 ECHR Compliant And Foreseeable Surveillance: The ECTHR's Expanded Legality Requirement Copied By The CJEU. A Discussion Of European Surveillance Case Law' [2020] SSRN Electronic Journal.
63. 'History Of Privacy Timeline / Safecomputing.Umich.Edu' (*Safecomputing.umich.edu*) <https://safecomputing.umich.edu/privacy/history-of-privacy-timeline> accessed 15 November 2021.
64. 'History Of Privacy Timeline / Safecomputing.Umich.Edu' (*Safecomputing.umich.edu*) <https://safecomputing.umich.edu/privacy/history-of-privacy-timeline> accessed 15 November 2021.
65. Hörnle J, 'How To Control Interception-Does The UK Strike The Right Balance?' (2010) 26 Computer Law & Security Review.
66. 'How Bulk Interception Works' (*Privacy International*, 2022) <https://privacyinternational.org/long-read/827/how-bulk-interception-works> accessed 8 February 2022
67. Howie E, 'Protecting The Human Right To Freedom Of Expression In International Law' (2017) 20 International Journal of Speech-Language Pathology
68. Howie E, 'Protecting The Human Right To Freedom Of Expression In International Law' (2017) 20 International Journal of Speech-Language Pathology
69. Ibid.
70. 'Intelligence Sharing In A Complicated World: The Future Of Five Eyes' (*The Cipher Brief*, 2021) <https://www.thecipherbrief.com/intelligence-sharing-in-a-complicated-world-the-future-of-five-eyes> accessed 13 November 2021.
71. 'Interception Of Communications Code Of Practice Pursuant To Section 71 Of The Regulation Of Investigatory Powers Act 2000' (*Assets.publishing.service.gov.uk*, 2016)

72. 'Interception, Investigatory Powers Act Factsheet' <https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/03/Interception.pdf> accessed 27 March 2022
73. 'Interim Measures' (Echr.coe.int, 2022) <https://www.echr.coe.int/Documents/Interim_Measures_ENG.pdf> accessed 22 March 2022.
74. 'Investigatory Powers Bill, Factsheet – Bulk Interception' (*Assets.publishing.service.gov.uk*) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473751/Factsheet-Bulk_Interception.pdf> accessed 8 February 2022.
75. Joergensen R.F., 'Can Human Rights Law Bend Mass Surveillance?' (2014) 3 Internet Policy Review.
76. Karsai Dániel, 'The Friendly Settlement Procedure And The ECHR | Karsai Dániel Ügyvédi Iroda' (Karsai Dániel ügyvédi iroda, 2022) <https://drkarsai.hu/en/friendly-settlement-procedure/> accessed 22 March 2022.
77. Kim S and others, 'New U.K. Law Fails European Court Standards On Mass Interception Disclosed By Snowden - Just Security' (*Just Security*, 2018) <https://www.justsecurity.org/60878/u-k-law-fails-european-court-standards-mass-interception-snowden-disclosed/> accessed 9 November 2021.
78. Lubin A, "Big Brother Watch v. UK (Eur. Ct. H.R. Grand Chamber)" [2022] International Legal Materials 1
79. MacAskill E and others, 'GCHQ Taps Fibre-Optic Cables For Secret Access To World's Communications' (*the Guardian*, 2013) <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> accessed 9 November 2021.
80. Malagutti M, '"Bulk Data: Intelligence And Surveillance."' [2018] Academia.
81. Matney L, 'Techcrunch Is Part Of The Yahoo Family Of Brands' (*Techcrunch.com*, 2015) <https://techcrunch.com/2015/08/03/uncovering-echelon-the-top-secret-nsa-program-that-has-been-watching-you-your-entire-life/> accessed 13 November 2021
82. Matney L, 'Techcrunch Is Part Of The Yahoo Family Of Brands' (*Techcrunch.com*, 2015) <https://techcrunch.com/2015/08/03/uncovering-echelon-the-top-secret-nsa-program-that-has-been-watching-you-your-entire-life/> accessed 13 November 2021.

83. Milanovic M and others, 'Ecthr Judgment In Big Brother Watch V. UK' (*Ejiltalk.org*, 2022) <https://www.ejiltalk.org/ecthr-judgment-in-big-brother-watch-v-uk/> accessed 2 February 2022.
84. Murray D and Fussey P, “Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data” (2019) 52 Israel Law Review 31.
85. Murray D and Fussey P, 'Bulk Surveillance In The Digital Age: Rethinking The Human Rights Law Approach To Bulk Monitoring Of Communications Data' (2019) 52 Israel Law Review.
86. NSA Glossary, '<Hr Style="Height:1Px;Border-Width:0;Color:Gray;Background-Color:Gray;">NSA Glossary' (*Electrospaces.net*, 2022) <https://www.electrospaces.net/p/glossary.html#:~:text=Strong%20Selector%20%2D%20A%20specific%20identifier,an%20AppProcIP%20or%20an%20AppProcMac%20*> accessed 7 February 2022.
87. Octavian Ichim, Just Satisfaction Under The European Convention On Human Rights (1st edn, Cambridge University Press 2015) p.11
88. Octavian Ichim, Just Satisfaction Under The European Convention On Human Rights (1st edn, Cambridge University Press 2015) p.181
89. Pepper D.S., 'The Business Of Sigint' (2010) 25 Public Policy and Administration.
90. Perrone J, 'The Echelon Spy Network' (*the Guardian*, 2001) <https://www.theguardian.com/world/2001/may/29/qanda.janeperrone> accessed 13 November 2021.
91. PETER G, “The Intelligence and Security Committee and the Challenge of Security Networks” (2009) 35 Review of International Studies 929
92. Peter Kempees, "Hard Power" And The European Convention On Human Rights (Brill 2020). p.225
93. Power D. J., Heavin C, and O’Connor Y, 'Balancing Privacy Rights And Surveillance Analytics: A Decision Process Guide' (2021) 4 Journal of Business Analytics.
94. 'Practice Direction: Requests Of Interim Measures (Rule 39 Of The Rules Of Court)' (Echr.coe.int, 2022) <https://www.echr.coe.int/Documents/PD_interim_measures_intro_ENG.pdf> accessed 24 March 2022.

95. 'PRIVACY AND SECURITY INQUIRY: OPENING STATEMENT' (*Isc.independent.gov.uk*, 2015) <https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312-ISC-PS-opening-statementweb.pdf> accessed 8 February 2022.
96. Randall M.H., 'Freedom of Expression in the Internet' (2016) 26 Swiss Rev Int'l & Eur L 235
97. Regulation of Investigatory Powers Act 2000, s 16(1)
98. Regulation of Investigatory Powers Act 2000, s 16(2)
99. Regulation of Investigatory Powers Act 2000, s 5(3)
100. Regulation of Investigatory Powers Act 2000, s 8(4).
101. Regulation of Investigatory Powers Act 2000, s 8(5)(a).
102. Regulation of Investigatory Powers Act 2000, s 81(1).
103. 'Regulation Of Investigatory Powers Act 2000/Part I - ORG Wiki' (*Wiki.openrightsgroup.org*) <https://wiki.openrightsgroup.org/wiki/Regulation_of_Investigatory_Powers_Act_2000/Part_I> accessed 6 February 2022.
104. 'Regulation Of Investigatory Powers Under RIPA 2000 | Legal Guidance | Lexisnexis' (*Lexisnexis.co.uk*) <https://www.lexisnexis.co.uk/legal/guidance/regulation-of-investigatory-powers-interception-of-communications-under-ripa-2000> accessed 10 November 2021.
105. Rollenhagen L, 'Alan Westin Is The Father Of Modern Data Privacy Law | Osano' (*Osano*, 2020) <https://www.osano.com/articles/alan-westin> accessed 15 November 2021.
106. Rosenzweig P, 'Surveillance Technology And The Rule Of Law' (*The Great Courses Daily*, 2021) <https://www.thegreatcoursesdaily.com/surveillance-technology-and-the-rule-of-law/> accessed 20 March 2022
107. 'Rules Of Court Rule 62§2' (Echr.coe.int, 2019) <https://www.echr.coe.int/Documents/Rules_Court_ENG.pdf> accessed 22 March 2022
108. Schermer B, *Software Agents, Surveillance, And The Right To Privacy: A Legislative Framework For Agent-Enabled Surveillance (SIKS Dissertation Series, 1873-0760 ; No. 2007-05)* (Amsterdam University Press 2007)
109. Schmahl S and Breuer M, The Council Of Europe Its Law And Policies (1st edn, Oxford University Press 2017) p.3

110. Schmahl S and Breuer M, The Council Of Europe Its Law And Policies (1st edn, Oxford University Press 2017) p.28

111. Schulhofer S.J., 'An International Right To Privacy? Be Careful What You Wish For' (2016) 14 International Journal of Constitutional Law.

112. Sharma C, 'Summary: Big Brother Watch And Others V. The United Kingdom' (*Lawfare*, 2018) <https://www.lawfareblog.com/summary-big-brother-watch-and-others-v-united-kingdom> accessed 2 December 2021.

113. Taylor N, 'State Surveillance And The Right To Privacy.' (2002) 1 Surveillance & Society

114. Taylor N, 'State Surveillance And The Right To Privacy.' (2002) 1 Surveillance & Society.

115. Taylor R.C., 'Intelligence-Sharing Agreements & International Data Protection: Avoiding a Global Surveillance State' (2018) 17 Wash U Global Stud L Rev 731

116. Taylor R.N., 'Not So Secret: Deal At The Heart Of UK-US Intelligence' (*the Guardian*, 2010) <https://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released> accessed 13 November 2021.

117. Thowsen M and Roy Krøvel, *Making Transparency Possible* (2019).

118. Townend J, 'Freedom Of Expression And The Chilling Effect' (*Academia.edu*, 2022) <https://www.academia.edu/34350408/Freedom_of_Expression_and_the_Chilling_Effect> accessed 16 February 2022.

119. Tzanou M, 'Big Brother Watch And Others V. The United Kingdom: A Victory Of Human Rights Over Modern Digital Surveillance?' (*Verfassungsblog*, 2018) <https://verfassungsblog.de/big-brother-watch-and-others-v-the-united-kingdom-a-victory-of-human-rights-over-modern-digital-surveillance/> accessed 2 March 2022.

120. UNGA Res 68/167 (18 December 2013) UN Doc A/RES/68/167

121. Universal Declaration of Human Rights(UDHR) art 12

122. Universal Declaration of Human Rights(UDHR) art 19

123. van der Sloot B and Kosta E, 'Big Brother Watch And Others V UK: Lessons From The Latest Strasbourg Ruling On Bulk Surveillance' (2019) 5 European Data Protection Law Review

124. Vermeulen J, 'Big Brother May Continue Watching You' [2018] Ghent: Human Rights Centre <https://biblio.ugent.be/publication/8612719> accessed 15 February 2022.

125. Vincent J, 'UK's Online Spying Habits Are Legal But Require Overhaul, Says Government' (*The Verge*, 2015) <https://www.theverge.com/2015/3/12/8198785/gchq-mass-surveillance-isc-report-2015> accessed 8 February 2022.

126. Vlahou A, 'Data Sharing Under The General Data Protection Regulation' (2021) 77 Hypertension <https://www.ahajournals.org/doi/10.1161/HYPERTENSIONAHA.120.16340> accessed 15 November 2021

127. Voorhoof D, 'Case Law, Strasbourg: Big Brother Watch V United Kingdom, Bulk Interception Regime Violated Articles 8 And 10 – Dirk Voorhoof' (*Inforrm's Blog*, 2021) <https://inforrm.org/2021/06/09/case-law-strasboug-big-brother-watch-v-united-kingdom-bulk-interception-regime-violated-articles-8-and-10-dirk-voorhoof/> accessed 2 December 2021

128. Walby K, 'Review Of Friedewald, Michael, J. Peter Burgess, Johann Čas, Rocco Bellanova, And Walter Peissl. (Eds). Surveillance, Privacy, And Security: Citizens' Perspectives' (2018) 31 Security Journal.

129. Waranch R.S., 'Digital Rights Ireland Deja Vu: Why the Bulk Acquisition Warrant Provisions of the Investigatory Powers Act 2016 Are Incompatible with the Charter of Fundamental Rights of the European Union' (2017) 50 Geo Wash Int'l L Rev 209

130. Warren S.D. and Brandeis L.D., 'Warren, Samuel & Louis Brandeis. The Right To Privacy, 4 Harv. L. Rev. 193 (1890)' (1890) 25 Communication Law and Policy.

131. Westin A.F., 'Science, Privacy, And Freedom: Issues And Proposals For The 1970'S. Part I--The Current Impact Of Surveillance On Privacy' (1966) 66 Columbia Law Review

132. 'What Is A Request For An Advisory Opinion?' (Echr.coe.int, 2022) <https://www.echr.coe.int/Documents/Press_Q_A_Advisory_opinion_ENG.PDF> accessed 24 March 2022.

133. 'WHAT IS FREEDOM OF EXPRESSION' (*Freedom Forum Institute*, 2022) <https://www.freedomforuminstitute.org/about/faq/what-is-freedom-of-expression/> accessed 9 March 2022

134. 'What Is Metadata (With Examples) - Data Terminology' (*Dataedo.com*, 2022) <https://dataedo.com/kb/data-glossary/what-is-metadata> accessed 8 February 2022.

135. 'What Is The European Convention On Human Rights?' (Amnesty.org.uk, 2022) <https://www.amnesty.org.uk/> accessed 10 March 2022

136. Zimmer M, 'Introduction: The “Privacy” Special Issue Of The Journal Of Intellectual Freedom & Privacy' (2017) 2 Journal of Intellectual Freedom & Privacy

137. Zwart M, Humphreys S, and Dissel B.V., 'Surveillance, Big Data and Democracy: Lessons for Australia from the US and UK' (2014) 37 UNSWLJ 713

