Volume 6, Number 2, Winter 2022–23

Mass Surveillance and the Right to Privacy

The approach of the European Court of Human Rights on Surveillance and the Right to Privacy

Elena-Mathilde Heiring*

This paper examines the development of the European Court of Human Rights (ECtHR) case law on the area of mass surveillance and bulk interception. First, by assessing what is enshrined within the right to privacy and what concerns are to be approached by the legislators and legal entities such as the ECtHR. The privacy concerns in the digital age concerning mass surveillance are presented briefly to map out why it is essential for the ECtHR to progress in its jurisprudence. To analyse and discuss the ECtHR's development concurrently with the advancements of technology, its early case law is explored and later the most recent case law of the past decade. The paper then critically analyses the ECtHR's recent findings of safeguards towards mass surveillance of communications in the case of *Big Brother Watch and Others v. United Kingdom*. It then concludes that the ECtHR's assessment provides proper standards in relation to mass surveillance but fails to approach whether the States' benefits of bulk interception in the form of national security outweigh the invasion of privacy of the affected individuals.

1. Introduction

Technology is a push for positive change in society, but the more we depend on it, the more data we generate. That is why the privacy of one's personal data has become such a critical concern; while users demand it, governments enforce it, and companies apply it to their strategies. The increased digitalisation of our

* LLM Student, University of Copenhagen [elenamheiring@gmail.com]

daily lives has a significant effect on the protection and respect of our Human Rights.

After the events of 9/11 and subsequent attacks in Europe, mass surveillance was enacted to protect Western democracies from the prominent threat of terrorism. As the surveillance of citizens and modern technologies continue to develop and introduce new opportunities and risks, which is far from a novel fact, it is crucial for Article 8 to remain relevant and capable of responding to increasingly complex capabilities. Hence it is strictly necessary for the ECtHR to similarly enhance the principles and minimum safeguards set forward by its caselaw. The ECtHR has developed an important set of principles and minimum safeguards to govern secret surveillance of communications in its case law on Article 8 of the European Convention on Human Rights (ECHR). These safeguards have played an essential role in shaping data privacy standards within Europe. This paper explains the standards of the right to privacy within the ECHR and then critically examines the development of the ECtHR's approach to the principles and safeguards posed by Article 8 ECHR. The last section provides an assessment on how the ECtHR has applied these data privacy standards specifically to secret surveillance measures.

2. Research Question

How does the European Court of Human Rights case law impact the human right to privacy, and in what way does it provide an adequate legal basis for the protection of the right to privacy in the online world?

3. Methodology

The paper aims to thoroughly examine the current human rights protection of privacy online, focused on the practice of the ECtHR. Furthermore, it will provide an in-depth discussion of the efficiency of the current ECtHR case law on surveillance and possible remedies. For this study, a literature review via desk research was conducted as the primary step by reading books, journal articles, and other online sources. This review aims to map the law consisting of the relevant legal instruments and relevant case law. A further examination of these human rights laws and cases requires the legal doctrinal method. The doctrinal method aims to gather, organise, and describe the current legal framework. Once

the relevant human rights rules are known, the paper can identify ambiguities, criticisms, and solutions. Additionally, qualitative legal research aims to untangle the workings of legal, social, and cultural processes, which is highly relevant to the paper's focus on how surveillance may continuously breach the human rights of individuals.

4. The Human Right to Privacy

4.1 Standards of the Human Right to Privacy

The right to privacy is a universal human right protected in several international, regional, and national laws, conventions, and treaties. Most notably, it is enshrined in one of the foundations of international human rights law; Article 12 of the United Nations Universal Declaration of Human Rights (UNDHR),

> 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.[1]

Similarly, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) mentions the protection of the right to privacy and Article 8 of the ECHR which will be discussed further in this paper.[2]

The right to privacy enables individuals to create their own private space and protects them from any unjustified and unwarranted interference or disturbance in their lives.

Although there is no universal notion of the human right to privacy, it is often associated with the ability to exercise control over one's personal information and generally protects against arbitrary and unjustified use of power by States. As a general principle, human rights are universal, and interpretations

[1] Universal Declaration of Human Rights (adopted 10 December 1948) (UDHR), art. 12.

[2] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) (ICCPR), art. 17; Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), art. 8.

by expert bodies and national courts have eventually generated a relatively consistent frame of international law on the right to privacy. However, the need for understanding and clarity of the human right to privacy is growing rapidly in response to individuals being increasingly connected to the online world, in which data gradually travels national boundaries. As the need to develop the standards of the right to privacy grows, the question becomes; where should the protection of the human right to privacy online go from here? This paper will solemnly examine the right to privacy in the scope of the ECHR.

4.2 Concerns about the Human Right to Privacy Online

Mass surveillance can subject people to indiscriminate monitoring while interfering with people's right to privacy, and the rights that privacy enables, such as the freedom of expression. The Snowden revelations in 2013 demonstrated an extraordinary scale of government mass surveillance programmes; surveillance programmes which constituted an intrusion into private lives all over the world. These revelations of the intrusive governance surveillance caused the frameworks for lawful access to be pressured and revealed the need of a rigorous internationally coordinated update. The reveal of details about the usage of pervasive surveillance technology only heightened anxieties about the loss of privacy. The first United Nations Human Rights Council (UNHRC) report on digital privacy after the Snowden revelations noted that:

> digital platforms were vulnerable to surveillance, interception and data collection […] Surveillance practices could have a very real impact on people's human rights, including their rights to privacy [and] to freedom of expression […] In particular, information collected through digital surveillance had been used to target dissidents and there were credible reports suggesting that digital technologies had been used to gather information that led to torture and other forms of ill treatment.[3]

[3] Human Rights Council, *Summary of the Human Rights Council panel discussion on the right to privacy in the digital age* (2014), page 3, para. 6.

The UNHRC report provides examples of the risks posed by surveillance technologies and underlines the newfound importance of protecting the right to privacy in order to protect other political freedoms.

The years following the Snowden revelations have been highly focused on how to protect the right to privacy online as well as offline, however, the Office of the High Commissioner argued in a UN special rapporteur in 2018 that it is impossible to protect the same rights online as are a given offline; "when dealing with technologies such as the internet, it is simplistic and naïve to be content with a statement that 'whatever is protected offline is protected online'".[4] Nonetheless, the UNHRC stated in its latest report in 2021 that "the same rights that people have offline must also be protected online, including the right to privacy".[5]

They additionally note that the increasingly obscure limit between the offline and online space can affect the individual's right to privacy; hence breaches of privacy online may have a severe effect even on the individual's rights offline.[6] This clearly shows how existing human rights are becoming relevant for the whole extent of human activity online.

The discussion proceeds to legal literature, and certain scholars have argued that the current international human rights framework is no longer designed to deal with the scenarios we face online. For example, Shany and Dror-Shpoliansky argue that cyberspace's unique features raise the question of whether extending offline human rights to the online world is desirable.[7] One of the reasons is that non-state actors play a significant role in constructing and operating within cyberspace, whereas States occupy the physical space in which the current human rights framework was created.[8] Hence new interests and needs present themselves, and the previous challenges of the offline world will evolve into new implications

[4] Special Rapporteur on the Right to Privacy*, Report on Security and Surveillance* (2018), page 25, para. 6.
[5] Human Rights Council, *Resolution on right to privacy in the digital age* (2021), page 2.
[6] Human Rights Council, *Resolution on right to privacy in the digital age* (2021), page 2.
[7] Dror-Shpoliansky, D. and Shany, Y. *"End as we Know it",* page 33.
[8] *Ibid.*, page 4.

While mass surveillance is not a new concept, it has evolved rapidly over the years, which has led to an industry focused on technological advancements designed for the purpose of mass surveillance. One of the most recent examples is the automation of face recognition that has been suggested in public spaces for optimising, for example, border control.[9] The European Parliament raises concerns about the risk of discrimination and surveillance of people who are not suspected of a crime.[10] It is evident that embracing technology in a responsible way is essential for the protection of the right to privacy.

5. The European Convention on Human Rights and the Right to Privacy

5.1 Scope of Article 8(1) of the European Convention on Human Rights

The ECtHR was created following the Second World War to guarantee the safeguard of certain rights and freedoms of the ECHR.[11] Article 8 of the Convention places an obligation on the contracting States to respect and protect specific personal interests and is written down as follows: [12]

(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.[13]

---

[9] Glusac, E. *"What You Need to Know About Facial Recognition at Airports"* (2022).
[10] European Parliament Press Release, "*Use of artificial intelligence by the police: MEP oppose mass surveillance"* (2021).
[11] Harris et al. *"Law of the European Convention on Human Rights"* (2018), pages 3-4.
[12] *Ibid*, page 501.
[13] ECHR, *supra* note 2, Article 8.

The framework on the freedom of privacy is summarised in the first section of article 8, by which the freedom protects an individual's private life, family life, home, and confidentiality of correspondence. However, like certain other rights under the ECHR, the second paragraph clearly states that the right to respect for private life is not absolute, and public authorities may intervene within specific requirements. The right to private life is a notion too broad to define fully, which is illustrated through the dynamic interpretation of Article 8 by the ECtHR.[14] The Court has interpreted the scope broadly under Article 8(1), considering social and technological developments to keep up to date with the emerging technologies and surveillance practices.[15] In the 1976 case *X v Iceland*, the Commission explained that the right to private life was not limited to privacy but also included the "right to establish and to develop relationships with other human beings, especially in the emotional field for the development and fulfilment of one's own personality".[16] Following the Commission's explanation in the 1976 case, the Court similarly stated in *Niemitz v Germany* which concerned the search of a lawyer's office, that "[…] it would be too restrictive to limit the notion to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings."[17] Consequently, the claims within Article 8 include any place where an individual's interaction with others is affected.[18]

The ECtHR guide on Article 8 provides three categories within the definition of "private life". First is the category of "physical, psychological or moral integrity", which includes issues such as victims of violence, forced medical treatment, reproductive rights, sexual life or orientation, and professional

[14] See for example the Court's statement in *Costello-Roberts v. the United Kingdom* (1993), para. 36.
[15] See for example *X v Germany* (1981), in which Article 8 was applied to a complaint regarding preservation of a police file, and thereby raised an issue of data protection. It was ruled to be within the broad scope of Article 8 ECHR, page 107.
[16] *X v. Iceland* (1976), page 87, para. 5.
[17] *Niemietz v. Germany* (1992), para. 29.
[18] Harris et al, *supra* note 11, page 504.

activities.[19] The second category is "identity and autonomy", which includes the right to personal development and autonomy, religious and philosophical convictions, gender identity, and ethnic identity.[20] Last is the category that incorporates the right to "privacy", concerning the right to one's photographs and image, protection of individual reputation and defamation, data protection, and access to personal information.[21] Privacy is the central aspect of this paper and will be examined below within the caselaw of the ECtHR.

5.2 Negative Obligations under Article 8 of the Convention

Article 8 of ECHR imposes both positive and negative obligations; hence the approach of the ECtHR depends on which type of obligation arises.[22] The positive obligation requires that the States take positive steps to protect the rights guaranteed under Article 8(1); however, it will not be treated further in this paper as it is of minimal relevance to the analysis of the ECtHR's approach to Article 8.

The latter imposes an obligation on States to avoid interference with any rights protected under Article 8 unless the conditions for justifying an interference are fulfilled. Most of the legal cases brought against surveillance measures under Article 8 concern negative obligations and are thus subject to a two-stage test.[23] The first stage considers whether the complaint is within the scope of Article 8(1). If the alleged interference is covered by Article 8(1), the Court will then examine whether the interference meets the conditions of Article 8(2). It is important to note that under the rule of law, governmental powers are limited by law and may be exercised only based on law, which provides that in order for a state to interfere with a user's privacy legally, the actions must meet

---

[19] The ECtHR, *Guide on Article 8 of the European Convention on Human Rights* (2021), page 30, para. 104.
[20] *Ibid*, page 60, para. 243.
[21] *Ibid*, pages 44-51.
[22] Akandji-Kombe, J-F. "*Positive Obligations under the European Convention on Human Rights*", page 10.
[23] Roagna, I. "*Protecting the right to respect for private and family life under the European Convention on Human Rights*", page 10; see also Feldman "*Civil Liberties and Human Rights",* page 665-667.

the terms of legality, necessity and proportionality. These requirements are written down in Article 8(2) of ECHR and Article 52 of the European Charter and are additionally confirmed in various cases by the ECtHR.[24] The three conditions of Article 8(2) are cumulative and must be complied with for a State to interfere. Since these requirements are cumulative, a failure to meet one of the three is enough to cause a violation of Article 8.[25] The first condition is the requirement of legality; any State intervention must be "in accordance with law".[26] Additionally, the legislation must contain foreseeability and accessibility as safeguards against arbitrariness in implementation.[27] Secondly, the intervention must pursue one of the several legitimate aims identified under Article 8(2). Finally, the measure must be proportional and "necessary in a democratic society"; nevertheless, adequate measures against abuse are still required.[28] When it comes to defining the margins of necessity, national authorities are granted a bit of leeway, as some cases can be very complex and sensitive; hence the national authorities may have a better position to evaluate each case in their circumstances and ascertain what direction is proper.[29] A further assessment of the necessity requirements will be examined below.

6. Case Law of the European Court of Human Rights on the Right to Privacy

6.1 Early Case Law

The ECtHR has gradually laid down specific requirements for contracting States' legal regimes to minimise the risk of arbitrary use of power. For example, in the landmark case *Klass v Germany* the Court found that the contested

[24] Council of the European Union, *Charter of Fundamental Rights of the European Union*, article 52; For rule of law cases see for example *Vavřička and Others v The Czech Republic*, para. 271 and *Big Brother Watch v United Kingdom* (2021), para. 332.

[25] Harris et al, *supra* note 11, page 511.

[26] Roagna, *supra* note 23, page 11.

[27] ECtHR, *supra* note 19, page 11, para. 18, and page 137, para. 629.

[28] The requirement of "necessary in a democratic society" was underlined by the ECtHR in *Zakharov v. Russia* (2015), para. 232.

[29] *Weber Saravia v Germany* (2006), para. 106.

domestic legislation founded a system of surveillance under which the communications of all individuals could be monitored. In other words, the Court established early in its caselaw that the scope of Article 8 ECHR included the rights of all those whose communications were monitored and who were not the primary focus of the surveillance.

As a result, an individual may claim to be the victim of secret surveillance based on its mere existence or on legislation permitting surveillance without having to provide evidence that such measures were applied to them. However, a complainant will have to establish a reason as to why such measures *may* apply to them and whether there has been an interference with their rights due to the possible threats posed by secret measures.[30] The Court later clarified in *Zakharov v Russia* that this possibility only applies in cases with no domestic remedies.[31] Recognising this status under Article 8 ECHR is ever more important given the significantly increasing use of bulk collection and surveillance regimes. The focus on adequate safeguards against abuse of power appeared in the two parallel cases of Kruslin and Huvig, in which the Court concluded that only some safeguards were provided for in law; hence the system did not provide adequate safeguards.[32] A few of the reasons cited by the Court concerned unclarity in the categories of people liable to have their phones tapped, absence of a limit on the duration of phone tapping, and unclarity about under what circumstance the recordings must be erased. The Court has continuously highlighted the requirements of the law to scrutinise surveillance.[33]

6.2 Recent Case Law

Following the legal and political fallout of the Snowden revelations, data retention and surveillance regimes have been subject to challenge and reform. An essential step in the ECtHR's practice was taken in 2015 in the judgment of *Zakharov v Russia* which revolved around secret surveillance of selected persons or groups. The Court made it clear that in cases of secret surveillance, where people generally are not aware that data gathering activities are targeting them,

[30] Harris et al, *supra* note 11, page 533.
[31] *Ibid*, page 534.
[32] *Kruslin v France* (1990), para. 45; and *Huvig v France* (1990), para. 34.
[33] See for example *Weber and Saravia v Germany*, *supra* note 29, paras. 94-95.

the principle of rejecting *in abstracto* claims could no longer be upheld.[34] Hence applicants may still claim to be victims of an interference violating Article 8 ECHR due to the mere existence of the surveillance practice without having to prove that such measures were applied to them. The Court clarified the importance of this measure with the following statement in the *Zakharov* case:

> in such circumstances the threat of surveillance can be claimed in itself to restrict free communication […], thereby constituting for all users, or potential users, a direct interference with the right guaranteed by Article 8. There is therefore a greater need for scrutiny by the Court, and an exception to the rule denying individuals the right to challenge a law in abstracto is justified. In such cases the individual does not need to demonstrate the existence of any risk that secret surveillance measures were applied to him.[35]

However, in cases where no exact period for review is specified, when the law and practice are examined *in abstracto*, the ECtHR Grand Chamber specified that the Court could not be expected to assess the "compatibility with the Convention before and after every single legislative amendment".[36] When the Court is examining bulk interception regimes *in abstracto*, and not how the laws have been applied at the material time, it primarily looks at the quality of the domestic regulatory framework without analysing its application in the specific case at hand.

The recent Grand Chamber judgment of *Big Brother Watch v United Kingdom* is highly relevant when mapping the scope of Article 8 ECHR. This case, as opposed to the *Zakharov* case, revolved around mass surveillance regimes, and while the claimant in *Zakharov* was a natural person, the *Big Brother Watch* case included both legal and natural persons. In both cases, the minimum

---

[34] *Zakharov v Russia, supra* note 28, para. 171.

[35] *Ibid*, para. 171; See also the continued statement: "By contrast, if the national system provides for effective remedies, a widespread suspicion of abuse is more difficult to justify. In such cases, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures."

[36] *Centrum för Rättvisa v Sweden* (2021), para. 150.

requirements of the law are linked to the requirement of "in accordance with the law" and particularly to the preamble of the ECHR, in which the requirements of proportionality and necessity in a democratic society are outlined:

> The "quality of law" in this sense implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when "necessary in a democratic society", in particular by providing for adequate and effective safeguards and guarantees against abuse.[37]

The Court follows this statement by outlining the minimum requirements set out to avoid abuses of power, which date back to the *Weber and Saravia* case.[38] Examples of the minimum requirements are a definition of the circumstances in which intercepted data may or must be erased and destroyed and the procedure to be followed for examining the data.[39] These minimum requirements to be upheld by States seem somewhat similar to privacy by design, which usually refers to an approach in systems engineering that aims to protect the users' privacy. It does so by the beginning of the development when integrating considerations of privacy issues. Similarly, the Court requires States to embed in their laws a certain standard to ensure that the management of personal data and privacy is kept to what is strictly necessary.

In the 2018 *Big Brother Watch* judgment, the dissenting judges Koskelo and Turković pleaded for a Grand Chamber (GC) decision, arguing that the assessment should not have been carried out based on criteria developed in outdated existing case-law such as *Weber and Saravia* (2006), as the global events, especially in a technological perspective, has developed drastically since the judgment was handed in 2006.[40] In the recent *Big Brother Watch* case the GC marks the end of a battle that started with the first *Big Brother Watch* case in 2013 following the Snowden revelations about the surveillance programs in

---

[37] *Big Brother Watch, supra* note 24, para. 334.
[38] *Weber and Saravia, supra* note 29, para. 95.
[39] *Big Brother Watch, supra* note 24, para. 335.
[40] *Weber and Saravia, supra* note 29; for the dissenting judges statement see the partly dissenting opinion in *Big Brother Watch v United Kingdom* (2018), para. 4.

the United States and United Kingdom. The GC agreed with the applicants that the United Kingdom's Regulation of Investigatory Powers Act (RIPA) failed to operate "in accordance with the law". However, the GC did not support the claim that the receipt of foreign intercept material violated the ECHR. The GC thus upheld the findings of the 2018 Chamber judgment that bulk interception by intelligence services is *per se* compatible with the ECHR, supported by the fact that bulk interception primarily is used for "foreign intelligence gathering, the early detection and investigation of cyber-attacks, counter-espionage and counter-terrorism".[41] Additionally, the Grand Chamber states that the internet is the most dangerous place and a platform for the "proliferation of threats that States currently face from networks of international actors, using the Internet both for communication and as a tool, and the existence of sophisticated technology which would enable these actors to avoid detection".[42] The partly dissenting judge Pinto de Albuquerque points out that these statements and arguments are not supported by any empirical evidence.[43] Similarly, the Grand Chamber recognised that its case law on bulk interception has to be further developed, which was illustrated when the end-to-end safeguards – originally developed in *Weber and Saravia* – evolved from a six-part to a new eight-part set of criteria.[44] The GC further outlines the "necessity" requirement, as it found that for an interference to be necessary and proportionate, there must be "end-to-end safeguards", such as an assessment of each stage of the process.[45] Consequently, it held that the legislation lacked the necessary safeguards and oversight measures to protect from abuse by the regime. Furthermore, the GC recognised that a wide margin still exists, within which the authorities can choose "how to best achieve the legitimate aim of protecting national security", but in contrast to previous judgments, added that "a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it".[46]

---

[41] *Big Brother Watch, supra* note 24, para 322.
[42] *Ibid,* para. 340.
[43] *Ibid,* partly dissenting opinion of judge Pinto de Albuquerque, para. 4 *ff.*
[44] *Big Brother Watch, supra* note 24, para. 361.
[45] *Ibid*, para. 361.
[46] *Ibid*, para. 339.

Through this judgment, the Court has put down a marker that state powers do not have a free hand with secret surveillance practice, as there needs to be much greater control of safeguards. It could be argued that with the somewhat sensible approach on *in abstracto* claims, the ECtHR is providing research on the most recent legal developments within surveillance technology in the contracting State. By doing so, the ECtHR contributes to the development of the newest standards for all members of the Council of Europe within an area that is rapidly evolving. However, this rather broad approach may potentially undermine the most important issue presented to the Court in defending the right to privacy, determining whether a disputed surveillance law amounts to a justified interference under Article 8(2) of the ECHR.

7. Assessing the Future of the European Court of Human Rights on the Right to Privacy

The ECtHR has, since the 1970s, developed several influential principles and safeguards governing secret surveillance under its Article 8 ECHR case law. However, concerns have been expressed regarding how the ECtHR has assessed whether mass surveillance is an appropriate tool in the 21st century and whether the Article 8 ECHR standards should be updated.

As demonstrated through the *Big Brother Watch* case at the Grand Chamber, the ECtHR might end up examining very different legal regimes for different periods, as regimes that were not compliant with Article 8 of the ECHR at the material time may inescapably evade any oversight or inspection by the ECtHR, resulting in few – if any – consequences for unsatisfactory State surveillance. This might send a deeply challenging message to public authorities who are granted extensive powers to use secret surveillance programs and collect significant amounts of data, as such powers by their very nature involve enormous risks of arbitrary abuse. Moreover, gaps in oversight may suggest that there is no meaningful assessment of whether Article 8 safeguards remain adequate and effective, thus encouraging a culture where public authorities believe they can perhaps act within a small field of immunity. Consider, for example, the Big Brother Watch case from 2018, first submitted to the ECtHR in 2013, just after the Snowden revelations. The ECtHR considered findings

from reports and legal challenges concerning surveillance programs delivered between 2013 and 2017.[47] This means that the Court did not have to consider whether the disputed system *had* been operating based on a clear, transparent, and foreseeable legal framework but rather whether it met the legality requirements at the time of the case in 2017. One would assume that where no specific time is given for what legal framework is to be examined, the ECtHR should apply the approach in which its examination is limited to the exact material time of when the disputed surveillance was in operation. An example of this approach is seen in the case of mass surveillance *Liberty v United Kingdom* from 2008.[48] The Court based the case on the Interception of Communications Act 1985 and deemed the breach of the legality condition a violation of Article 8 ECHR. Even so, the Court outlined legal reforms adopted *after* the material time of the dispute. However, it did so without combining its assessment of the different periods and legal frameworks and thus avoided any oversight gaps. The ECtHR thus managed to meet its progressive role of acknowledging any legal developments that could guide other contracting States when assessing the compliance of their national legal framework with Article 8 of ECHR. The Grand Chamber (GC) in the 2021 *Big Brother Watch* case seems to take an approach similar to the one in *Liberty*, as the judgment does not concern itself with the legality of the interception and the States' obligations under Article 8 ECHR but rather whether the means of the operation meet the necessary standards.

Overall, the Court provides some useful standards and safeguards in relation to mass surveillance and addresses the challenges of not only data but also metadata by stating that "any intrusion occasioned by the acquisition of related communications data will be magnified when they are obtained in bulk".[49] Additionally, the Court recognises that its jurisprudence from the past decade cannot stand the test of the internet innovation, in which "lives are increasingly

[47] *Big Brother Watch, supra* note 24, para. 1.

[48] *Liberty v United Kingdom* (2008), para. 34 *ff.*

[49] *Ibid,* para. 341; Metadata includes data left on the internet such as location information, author of the information, and other identifiers.

lived online".[50] The consequence of this statement is the extension of the end-to-end safeguards as bulk interception gets closer to the individual, the more advanced it becomes. In conclusion, the GC made reasonable advancements to protect the human right to privacy in the online environment; however, it arguably missed the opportunity to address the technology of the last decade, namely Big Data. The approach still seems to be based on the logic of surveillance, in which the protection of privacy increases the closer the surveillance is to the individual, meaning the more a camera closes on the individual, the more guarantees are required to protect the privacy. Nevertheless, the Big Data system resembles more of an infinite set of cameras installed in everything from public streets to private homes and pockets, which intelligence services can access on demand. This failure to recognise and effectively regulate the current risks of data gathering imperils the Court's capability to protect the human rights of people subject to bulk interception.

From the perspective of privacy and data protection the standard set by the GC is a rather thin one, as the Court endorsed mass-surveillance as acceptable, by upholding the findings of the previous judgment that mass surveillance by intelligence services is "*per se*" compatible with the ECHR. The decision reinforces the ECtHR's longstanding liberal approach to the possibility of governments deploying mass surveillance regimes, where certain procedural safeguards are incorporated. Even when those safeguards may be seen as a vague attempt to protect privacy. The GC neither engages with the broader question of whether the benefits of bulk interception outweigh the invasion of privacy of the affected individuals. It is more or less assumed that better-placed institutions within the contracting States have already made such determinations. Thus, the effect marker put down by the Court in the previously mentioned statement (note 51) is yet to be seen.

The possible consequences of this judgment are grave. One of the highest European jurisdictions accepts the removal of online anonymity for law enforcement purposes and mass surveillance by government authorities for national security purposes as a new normal. Following the GC's judgment on the *Big Brother Watch* case, the United Kingdom can now argue that it will easily

[50] *Ibid,* para. 341.

bring itself in line with the Strasbourg requirements and that its mass surveillance regime is, *per se,* not violating the Convention. Moreover, the judgment tends to fit the latest trend in Europe that instead of challenging or simply banning an intrusive intelligence measure at the outset, the trend is to allow it and then rather burden it with technical and procedural safeguards. Part of the judges, however, acknowledged some of the dangers of bulk interception as the judges Lemmens, Vehabović and Bošnjak warned that "in performing the balancing exercise, the majority have failed to assign proper weight to private life and correspondence which in several respect remain insufficiently protected in the face of interference by bulk interception".[51] On a similar but more alarming note, judge Pinto de Albuquerque notes in his dissenting opinion that "for good or ill, and I believe for ill more than for good, with the present judgment the Strasbourg Court has just opened the gates for an electronic 'Big Brother' in Europe". Judge Albuquerque also observed that it "fundamentally alters the existing balance in Europe between the right to respect for private life and public security interests in that it admits non-targeted surveillance"[52] Having said that, the GC did recognise that domestic law must contain specified rules on authorisation and circumstances in which communications must be intercepted.[53] However, mass surveillance of foreign communications was recognised in the judgment as an indispensable tool for states to safeguard national security. With the result of this case, the ECtHR has reaffirmed that bulk interception is here to stay.

The ECtHR is not the only legal organ within the EU that can, and attempts to, protect the right to privacy online. An example of a legal framework that is an excellent step for human rights is the EU Declaration on Digital Rights issued by the Commission to the European Parliament in January 2022.[54] The new principles call for democratic oversight of the digital society and economy, "in

[51] *Big Brother Watch, supra* note 24, partly dissenting opinion of judges Lemmens, Vehabović and Bošnjak, para. 30.

[52] Pinto de Albuquerque, *supra* note 43, paras. 60 and 59.

[53] *Big Brother Watch, supra* note 24, para. 348.

[54] European Commission "*Declaration on European Digital Rights and Principles"* (2022).

full respect of the rule of law principles, effective justice and law enforcement."[55] The declaration may guide legislators as they explore the possible implications of the continuous digital transformation or serve as a reference point for businesses as they expand and implement new technologies. Furthermore, the Commission highlights that the rights and freedoms enshrined in the EU's legal framework should be respected online as they are offline and thus put forward the necessary principles to ensure the protection of fundamental rights such as privacy. Essentially it establishes a framework to ensure that fundamental rights are a part of current and future digital policies. It is, of course, still unclear whether this proposal by the Commission will solemnly add to a declaration on digital rights such as the Lisbon declaration or if it will become a new digital pillar for the EU. Nevertheless, it is a small step in the right direction, and it is to be hoped that the ECtHR will follow a similar path and revisit its jurisprudence from the *Big Brother Watch* case in future cases to more effectively ensure that it provides efficient protection of human rights within the challenges of today's technologies and not those of the past.

8. A Judicial Dialogue on Data Retention Jurisprudence

The European Court of Justice (CJEU) has similarly delivered landmark cases concerning bulk data retention for national security purposes, most recently in *Privacy International* and *La Quadrature du Net.*[56] In these seminal decisions, the CJEU affirmed that bulk data retention laws for national security purposes fall within the scope of EU data protection law and presented the limitations and conditions under which permissible surveillance can be carried out. The data retention narrative of the CJEU commenced in 2014 with the case *Digital Rights Ireland*, in which the CJEU invalidated the Data Retention Directive as being incompatible with EU law.[57] In *Privacy International,* the CJEU maintains this expansive data protection jurisprudence by acknowledging the importance of

[55] *Ibid,* preamble, number 6.

[56] *Privacy International*, Case C-623/17 (CJEU 2020); *La Quadrature du Net*, Joined Cases C-511/18, C-512/18 and C-520/18 (CJEU 2020).

[57] *Digital Rights Ireland,* Case C-293/12 (CJEU 2014), para. 69.

national security purposes whilst maintaining the general prohibitory rule of indiscriminate bulk retention even when undertaken for national security purposes.[58]

Nevertheless, in *Quadrature du Net*, the CJEU departs from its prohibitive approach to bulk data retention and reaches a more nuanced one that allows for various diverse permissible surveillance measures if these are carried out under certain criteria and applicable safeguards. Additionally, *Quadrature du Net* maps out a hierarchy of legitimate public interests with national security at the top of the list, followed by combating serious crime and safeguarding public security; this is thus the first case developing a comprehensive assortment of permissible national data retention laws.[59] By the judgment of *Quadrature du Net,* the CJEU expands its assessment of data retention both vertically and horizontally to ensure European fundamental rights at a national level where data retention measures may be fragmented and vary between Member States. Contrary to the ECtHR's starting point in *Big Brother Watch,* which declares bulk interception regimes as "a valuable technological capacity to identify new threats in the digital domain", the CJEU maintained that bulk data retention, *per se*, is incompatible with fundamental rights.[60] Both Courts have prescribed several procedural guarantees regarding access and oversight, retention, and authorisation; however, contrary to the ECtHR's different stages of bulk interception processes in which the degree of interference increases as the process progresses, the CJEU views each step as a separate interference. Additionally, the CJEU started by declaring bulk data retention incompatible with fundamental rights, whereas the ECtHR's starting point provided a broader acceptance of bulk data retention.

Nevertheless, the Courts are currently not walking in different directions. The acceptance by the CJEU of the permissibility of bulk surveillance for national security purposes moves the Court closer to the case law of the ECtHR and could be seen as a reasonable approach aiming to make bulk surveillance an exception rather than the rule by ensuring national data retention regimes are subject to certain stringent criteria and safeguards. Both Courts demonstrate a

---

[58] *Privacy International, supra* note 56, para. 81.

[59] *Quadrature du Net, supra* note 56, para. 135.

[60] *Big Brother Watch, supra* note 24, para. 323.

more proceduralised approach to surveillance whilst backtracking from red lines and moving towards a more gradual acceptance, though within strict safeguards. Thus, the recent case law and the shift of the ECtHR, most notably in the recent *Big Brother Watch* case, signals a progressive re-alignment of the Courts, departing from previous case law. As the Courts harmonise their jurisprudence, it is to be hoped that the recent, more lenient approach of the ECtHR will not lead to a further downgrading of the stricter safeguards developed by the CJEU.

9. Conclusion

The digital technology era offers significant opportunities for a better quality of life, innovation, economic growth, and sustainability whilst also creating growing concerns and challenges for society's security, function, and stability.

The ECtHR outlined the framework of bulk interception of communications in the mid-2000s and elaborates on this policy line through the latest *Big Brother Watch* judgment, which will most likely be the guiding precedent for the ECtHR when confronted with cases on mass surveillance. The judgment aligns with the judicial thinking implemented through the *Liberty* and *Weber* cases but acknowledges a need to develop the case law further. The Court's judgment sets a precedent that State bodies should be transparent to their citizens; meanwhile, the latter's private life and communications should enjoy a guaranteed degree of privacy. The requirement that a secret surveillance system must provide adequate protection against abuse, including an independent supervisory body, is a strong message from the Court that will hopefully be seen in future judgments from Strasbourg. However, the Court's failure to truly develop any significant new requirements or identify where there is explicitly a need for new developments may be justified by the immense number of cases it has to process each year and, as a result, the tendency to apply already established principles when the disputing parties fail to provide a well-reasoned challenge. Despite people being willing to give up their privacy in exchange for some benefit here and now, they will not be able to control how that information will be used in the future. It is impossible to withdraw private information once it has been disclosed entirely.

We must be aware of the ethical threats to privacy in the digital age and realise that there is an urgent demand for transparency, accountability, and proportionality to meet the ethical issues that mass surveillance presents. Even

though citizens are protected by democratic rights and legislation such as the GDPR, it is crucial that there is greater protection from abuse of power. The prospects for privacy and data protection seem somewhat gloomy due to the latest Grand Chamber judgment. As of right now, the ECtHR does not prove to provide an adequate legal basis for the protection of the right to privacy from mass surveillance; however, it is yet to be seen if the dissenting statements of the Court and the potential legislation within the EU will bring new and more effective measures to the table. Perhaps in the future, the surveillance capitalists will be obliged by law to grant access to their data assets and allow users to customise their profiles used for ad targeting. Surveillance institutions are powerful entities, but they are not untouchable. They fear the law, lawmakers, and citizens who insist on a different path ahead. These are bound together in the pursuit of rescuing the digital future for the sake of democracy.