



Privacy and Freedom of Expression

Privacy and Freedom of Expression

Credits

Collection directors

Lee C. Bollinger

Catalina Botero-Marino

Editors

Juan Manuel Ospina, editor of the paper *Special Collection on the Case Law on Freedom of Expression: Privacy and Freedom of Expression*

Design

Vladimir Flórez (Vladdo), *illustrator*

Lourdes de Obaldía, *layout and graphic designer*

Special thanks

*Special thanks to Carlo Carvajal, José Ignacio Michaus, and Irene Parra for their collaboration on the paper *Special Collection on the Case Law on Freedom of Expression: Privacy and Freedom of Expression*.*

The Directors and Editors of the present collection would like to recognize and express their gratitude to all the people whose efforts and talents made the collection a reality. These publications were only possible thanks to the analysis and selection of cases for the database by a wide number of [experts](#) and [contributors](#) collaborating with Columbia Global Freedom of Expression. The case briefs presented in this collection reproduce the analysis of the cases published in our database, which was only possible due to their invaluable contribution.

Table of Contents

I.	Methodological clarifications	<i>7</i>
II.	Introduction	<i>9</i>
III.	Case Law	<i>11</i>
	A. Cases where privacy and free expression have a mutually reinforcing relationship	<i>11</i>
	i. National security and surveillance	<i>12</i>
	ii. Personal data in governmental databases	<i>12</i>
	iii. Data transmission to security and intelligence agencies from providers of electronic communication services	<i>13</i>
	iv. Data protection and internet platforms	<i>14</i>
	v. Requiring Internet Service Providers (ISPs) to store telecommunications data	<i>15</i>
	vi. National legislations establishing mass surveillance of electronic communications	<i>15</i>
	vii. Electronic espionage: Pegasus spyware	<i>16</i>
	viii. Interception of communications and access to phone records	<i>16</i>
	ix. Surveillance of foreign telecommunications	<i>18</i>
	x. COVID-19 Pandemic surveillance and data protection	<i>19</i>
	xi. Surveillance and tracking by private actors	<i>20</i>
	xii. Anonymity	<i>21</i>
	xiii. Publication of personal data by public agencies	<i>21</i>
	xiv. Compulsory registration in databases	<i>22</i>
	xv. Facial recognition	<i>23</i>
	xvi. Access to the internet, privacy, and freedom of expression	<i>24</i>
	xvii. Personal correspondence	<i>24</i>
	xviii. Protection of journalistic sources	<i>24</i>

B. Balancing the competing rights of privacy and freedom of expression	25
i. Public figures, privacy and public interest	25
ii. The duty to notify subjects before publishing articles concerning their private life	28
iii. Publication of private information of public interest available on the public dominion	29
iv. Publication of private photos from social media not directly related to matters of public interest	29
v. Radio broadcast of a private conversation of public interest	29
vi. Publication of health-related information about public officials	30
vii. Publications about people with HIV	30
viii. Information about patients in psychiatric hospitals	31
ix. Publication of images of a public official	32
x. Private images or information of no public interest	33
xi. Publications about a public official's family life	34
xii. Publications regarding accusations against public officials for sexual offenses	34
xiii. Publication of personal tax data without authorization of its owner	34
xiv. Classification of information regarding the impeachment of judges	35
xv. Public officials' personal information contained in official records	35
xvi. Salaries of public officials	37
xvii. Consumer Privacy	37
xviii. Rights of children	37
xix. Privacy and public interest in the reporting of criminal cases	39

I. Methodological clarifications

The rights to freedom of expression and privacy are recognized in a wide range of universal and regional international treaties. Articles 12 and 19 of the [Universal Declaration of Human Rights](#) respectively recognize the rights to privacy and freedom of expression, as do Articles 17 and 19 of the [International Covenant on Civil and Political Rights](#). At the regional level, the [European Convention on Human Rights](#) (“ECHR”) recognizes both rights in Articles 8 (privacy) and 10 (freedom of expression), whereas the [American Convention on Human Rights](#) does the same in Articles 11 and 13. In the same vein, both rights are recognized at a national level by numerous constitutions in regions across the world. According to the [Constitute Project](#), [192 countries](#) include the right to freedom of expression in their constitutions, while [183](#) do the same for the right to privacy.

As part of the *Special Collection of the Case Law of Freedom of Expression*, the purpose of this paper is to present, in a systematic manner, the summaries of some of the landmark decisions from different regional and national jurisdictions that are found in the Columbia Global Freedom of Expression database. The paper serves as an illustrative summary of emblematic decisions that may be of interest to judges, lawyers, and activists. It is our aim—through the systematization of the case analysis included in our database—to present the diverse case law of different legal systems about privacy and freedom of expression, their mutually reinforcing relationship, and the tensions that have arisen when these rights collide.

That said, our paper is not meant to be a comprehensive or exhaustive list, nor a comparative study: it is meant to be a short reference document that serves as a brief introduction to what is systematized in our database and to how different courts have resolved highly contentious matters at the present time. The comparative global study of case law about the tension between the right to freedom of expression and the right to privacy could fill entire volumes since this is an extraordinarily prolific field in the jurisprudence of both national and regional courts. Furthermore, the way these cases have been resolved by different courts is closely related to the varying legal cultures of each jurisdiction and their understanding of the concept of constitutional democracy. A comprehensive comparative study would have to consider these differences.

The purpose of this paper is to present, in a systematic manner, the summaries of some of the landmark decisions from different regional and national jurisdictions that are found in the Columbia Global Freedom of Expression database.

It is important to note that the paper includes decisions from both regional human rights courts and national high courts. In some cases, however, due to the novelty or the importance of some rulings, we included decisions from first instance, appellate, and specialized courts from a wide number of jurisdictions. It is also true that, in some cases, tribunals in different jurisdictions have arrived at different alternative solutions. For this document, we have chosen the decisions we consider to be of the utmost interest for the following reasons: they conform more clearly to global standards and

trends; they show the complexity of the tensions to be resolved; or, given their degree of arbitrariness, it is important to highlight them by way of contrast.

Following the format used in the *Special Collection of the Case Law of Freedom of Expression*, most of the cases in the paper do not include or explain the criteria that judges used to come to their decisions. The paper presents each case's summary as it appears in the analysis in our database – the analyses which our network of [researchers](#) and [experts](#) contribute to. These summaries briefly explain the relevant facts of the case and the legal resolution. Nevertheless, each case includes a link to its more comprehensive analysis found in our database, which includes a more detailed description of the facts of the case; the arguments of the court, tribunal, or judge; a list of references of international standards —or other decisions— cited by the ruling; an evaluation of the decision in terms of its impact and relevance regarding freedom of expression; and a link to the original document, among other resources.

For this paper, our internal team reviewed more than 240 decisions from different courts and selected those they considered to be most significant, taking into account the importance of having a diverse sample. Space restrictions limited this difficult selection process and meant that rulings of great impact had to be left out. Nevertheless, readers will find some of the most emblematic cases from regional human rights courts, in addition to relevant cases from national courts in the Global North and South.

Once the final selections were made, we defined our criteria for systematizing the cases and assigned them to their appropriate section. This will allow readers to quickly identify and locate any particular decision of their interest. In any case, on the Columbia Global Freedom of Expression website, users can use our thematic search engine to locate other decisions on their topic of interest and find a more extensive list of cases. As mentioned previously, this paper is an introduction to the significant resources found on our website.

The body of the paper is divided into two main categories: those cases where privacy and freedom of expression mutually reinforce one another, and those cases where privacy and freedom of expression are in conflict. Subsequently, each of the two main categories is divided into thematic subsections, highlighting the broad scope of issues discussed under the privacy/freedom of expression paradigm.

As mentioned above, each judgment will have the name of the case (as titled by Columbia Global Freedom of Expression), a summary of the decision, and a direct link to its complete analysis in the Global Freedom of Expression case law database. We hope this helps readers easily access some of the more relevant cases within specific themes, while also showing a small sample of the jurisdictional diversity of the case law. It is important to note that certain cases could be classified under more than one category. For the purpose of the paper, we categorized them in such a way as to present the broadest scope of themes reasonably possible. To see what other themes a particular judgment might address, we invite readers to visit our case law database. Case analyses can be accessed by clicking the link at the end of each case summary.

II. Introduction

The right to freedom of expression has been described by the ECtHR—in the case of *Von Hannover v. Germany (No. 2)*—as “...one of the essential foundations of a democratic society and one of the basic conditions for its progress and for each individual’s self-fulfillment”. However, as with any right, it is subject to limitations. In any case, any interference with this right, to be legitimate, must be prescribed by law, pursue a legitimate aim, and be necessary and proportionate, in the context of a democratic society, to achieve its aim. One of the legitimate aims that may justify the limitation of freedom of expression—as long as the other criteria are met—is the right to privacy.

Privacy has been defined by the IACtHR—in *Fontevicchia and D’amico v. Argentina*— as a fundamental right that guarantees “being free and immune to invasions or abusive or arbitrary attacks by third parties or public authority and may include, among other dimensions, the freedom to make decisions related to various areas of a person’s life, a peaceful personal space, the option of reserving certain aspects of private life, and control of the dissemination of personal information to the public”.

The border between a robust exercise of freedom of expression and proper protection of the right to privacy has been a matter of intense judicial scrutiny by numerous courts around the world. This paper aims to provide a brief outlook on how the protection of privacy by courts can also reinforce the protection of freedom of expression, and the case law where the protection of privacy has come into conflict with the exercise of such right.

The border between a robust exercise of freedom of expression and proper protection of the right to privacy has been a matter of intense judicial scrutiny by numerous courts around the world.

In this paper, we have decided to include emblematic cases about the protection of privacy, that although do not explicitly analyze freedom of expression, provide robust protection to the aforementioned right due to the interdependence between privacy and freedom of expression. For instance, in cases where courts have acknowledged the negative impact of systems of mass surveillance, or overly broad data collection, on the right to privacy, the scope of freedom of expression expanded too, by providing an advantageous legal framework against the potential chilling effect that constant or large-scale vigilance has on citizens, among other things. In fact, the reader will be able to learn from this paper that worldwide case law on the protection of the right to privacy from indiscriminate communication surveillance, has become fundamental to the free exercise of speech, particularly for critical journalism and public debate.

Other areas where the protection of privacy reinforces freedom of expression are the protection

of anonymity in expression and the use of the public interest doctrine. In both areas, the protection of privacy can be interpreted as a safeguard for robust and more uninhibited expression.

In contrast, it is also true that, when these rights collide, the balancing exercise inevitably triggers the prevalence of one right and the restriction of the other. These are often more difficult cases, in which international standards can be used as a guide to adopt a decision. As a matter of fact, the tension between these rights does not necessarily imply a negative outcome *per se*. It merely highlights that there are circumstances where the scope of the right to freedom of expression or privacy has been legitimately subject to limitations. Some examples of this can be found in this paper's categories related to personal information about public officials, the protection of health-related information, or the rights of children.

However, there are also judgments where the protection of one of these rights leads to the illegitimate sacrifice of the other. This can be seen in rulings that, for example, deny access to information about the salaries of public officials, without even considering the public interest such information entails. For more detailed information regarding the right of access to information, a future paper by Global Freedom of Expression will further analyze the case law on this topic.

The rise of information and communication technologies has caused the right to data protection to become an integral part of this debate. This right, recognized in several legislations and constitutions around the world in various degrees, and in Article 8 the Charter of Fundamental Rights of the European Union, has become central in shaping the relationship between expression and privacy in the digital sphere. The protection of personal data has also been subject to intense judicial activity. Although its content touches upon several aspects of autonomy, we will only focus on the rights related to privacy and freedom of expression.

Data protection as a fundamental right, as the case law shows, has both served to reinforce freedom of expression or come into direct conflict with it. On the one hand, data protection has enhanced freedom of expression by ensuring that the correct procurement, processing, and retention of personal information is not misused. This can be seen in decisions related to surveillance in the context of national security, the protection of citizens against facial recognition in public places, or the use of personal information to track the political activity of individuals. On the other hand, an expanding interpretation of the right has given rise to cases where imposing liability trumps the right to access information or limits the free exercise of journalism.

As a final note, we would like to make the reader aware of the fact that this paper will not analyze the discussion around the so-called right to be forgotten and the case law that arose after the *Costeja Case* before the Court of Justice of the European Union (CJUE) in 2014. This topic is analyzed in [another publication](#) that is part of this collection.

III. Case law

A. Cases where privacy and free expression have a mutually reinforcing relationship

In the following pages, we have systematized cases from different jurisdictions in which the protection of privacy has led to the protection of freedom of expression. Cases are ordered by topic, country, and court of origin. In most cases, the paper does not explain the criteria used by judges to solve them, since the document only systematizes the summaries of the cases in our database that were prepared by [researchers](#) and [experts](#) affiliated with our program. However, at the end of each case summary, we have included a link to the database entry of the case, in which it is possible to find a more detailed description of the facts of the case and the court's arguments, a list of references of the international standards and case law cited in the decision, an evaluation of the decision and the link to the original document, among other things.

i. National security and surveillance¹

ECtHR²: In the case of *Big Brother Watch and Others v. The United Kingdom (No. 2)* (2021), the Grand Chamber concluded that section 8(4) and Chapter II of the UK's Regulation of Investigatory Powers Act ("RIPA") had violated the rights to privacy and freedom of expression of the European Convention on Human Rights (Convention). The applicants argued about the compatibility of three electronic surveillance programs operated by the UK's Government Communications Headquarters (GCHQ) with the Convention. These programs were the following: (i) Bulk interception under the TEMPORA program, which stored and managed large volumes of data drawn from bearers; (ii) the intelligence-sharing regime with foreign countries, particularly the United States of America through the PRISM and Upstream programs; and, (iii) the procurement of communications data from communications service providers (CSPs). The three complaints were submitted after Edward Snowden's disclosures revealing surveillance programs managed by both the intelligence services of the United States of America and the United Kingdom. The Grand Chamber found that the UK's regimes on bulk interception and obtaining data from communications service providers had violated the Convention as the following deficiencies were detected: (i) the absence of independent authorization and oversight (the so-called "end-to-end safeguards"); (ii) no categories of selectors were included in the applications for a warrant; (iii) there was no prior internal approval of the selectors linked to an identifiable individual, and

¹ The following Courts have also analyzed the impact of national security and surveillance on the rights of freedom of expression and privacy: United States: *John Doe, Inc. v. Mukasey* (2008), Appellate Court. More info [here](#). Kenya: In the case of *Okoiti v. Communications Authority* (2018), First Instance Court. More info [here](#). United Kingdom: *Secretary of State for the Home Secretary v. Watson* (2018), Appellate Court. More info [here](#); *Davis v. Home Secretary* (2015), First Instance Court. More info [here](#).

² The following text, and the other case summaries here systematized, reproduces the summary and outcome section of the case analysis of this ruling included in our database, as made by experts and researchers affiliated to the program. The full text of the case analysis, and the original judgement, can be accessed through the link at the end.

(iv) the State did not examine other less intrusive measures before activating and implementing electronic surveillance programs, among other safeguards.

The judgment expands freedom of expression in the sense that some aspects of the UK’s mass surveillance regime were found unsuitable within the meaning of Article 10 of the Convention, particularly the Section 8(4) regime and Chapter II regime, previously discussed.

Nevertheless, the Chamber could have gone further in its duty to protect and promote freedom of expression. For instance, the Chamber admitted that the section 8(4) regime fell within the margin of appreciation of States since it did not intentionally target journalists. In other words, following the Grand Chamber’s criteria, mass surveillance measures, in general, are compatible with the Convention insofar as they are justified by an overriding requirement in the public interest and are accompanied by the corresponding legal safeguards, authorizations, and arrangements limiting the State Party’s ability to access privileged material.

The judgment expands freedom of expression in the sense that some aspects of the UK’s mass surveillance regime were found unsuitable.

Likewise, the Chamber noted that the Chapter II regime afforded enhanced protection where data were sought to identify a journalist’s source. However, this meant that any other journalistic information, as long as it does not involve journalistic sources, was left unprotected. In the instant case, since no specific provisions restricted the UK’s ability to access journalistic information when combating “serious crimes,” the Grand Chamber found that the Chapter II regime did not comply with Article 10 of the Convention. More info [here](#).

ii. Personal data in governmental databases

ECtHR: In the case of *M.D. and Others v. Spain* (2022), on June 28, 2022, the Third Chamber of the European Court of Human Rights (ECtHR) unanimously held that the compiling of files by the police in Catalonia on judges who had expressed views on that region’s independence from Spain infringed the judges’ right to privacy. The case concerned the compiling of files by the police in Catalonia on judges who participated in the authorship of a manifesto expressing that under the Constitution and international law, Catalan people should have a say on the region’s independence. Personal information and photographs were subsequently leaked to the press.

Following a complaint by the applicants, the Investigating Judge no. 15 of Madrid and the Audiencia Provincial dismissed their claims because there were sufficient grounds for attributing the leak to a particular person. Concurrently, disciplinary proceedings were brought against the applicants for signing the manifesto by the General Council of the Judiciary; however, no sanctions were issued, and the proceedings were closed.

In its decision, the ECtHR found that since there was no legal provision authorizing the compiling of such reports, their mere existence contravened Article 8 of the Convention. Regarding the

investigation into the leak, the Court found the national authorities had acted inadequately, particularly for failing to interview the Chief of Police of Barcelona, who was crucial to the investigation. Regarding the applicants' allegation that their right to freedom of expression had been infringed, the Court held that no sanction or chilling effect could be determined from the fact that disciplinary proceedings had taken place. More info [here](#).

In the case of *Catt v. United Kingdom* (2019), the European Court of Human Rights (ECtHR) found a violation of a peace activist's right to privacy in relation to personal data which had been collected and retained in an "extremist database" maintained by the police, despite him never having been assessed as a threat. The Court affirmed previous case law which found the broad collection of information to prevent crime and disorder to be lawful and pursue a legitimate purpose. However, in the present case, the retention of personal data without scheduled review and beyond established limits was disproportionate and unnecessary. The Court took issue with the domestic courts' failure to recognize the sensitive nature of some of the data retained on Catt, the applicant, namely data revealing his political opinions and affiliations with labor unions, which are subject to greater protections. It also called attention to the "ambiguous" nature of legal framework for the database and lack of appropriate safeguards to prevent abuse or arbitrariness.

In this decision the Court does not analyze the right to freedom of expression when considering the reasons for its ruling. Nonetheless, the scope of the protection of privacy in this particular case provides a protection to the right to freedom of expression against the chilling effect of surveillance or overly broad data collection. More info [here](#).

Colombia: In the case of *Mena v. ICETEX* (2013), the Constitutional Court of Colombia ruled that a state agency had violated the petitioner's fundamental rights by denying her access to its offices because she had previously participated in a peaceful protest in front of their building. The petitioner claimed that she was not allowed to enter the building out of racial discrimination, due to her Afro-Colombian origins. The Court found that the agency, rather than the building's management as asserted, had collected personal data on the petitioner after she participated in the protests. This violated the petitioner's habeas data and equality because she was neither informed of the real reason why she was denied access to the building nor of the existence of negative data as a result of her participation in the protest. In the opinion of the Court, the situation was further aggravated because the petitioner was also prevented from conducting legitimate business at the public agency. For all these reasons, the Court decided to protect the petitioner's fundamental rights and ordered the agency to publicly apologize for its inappropriate conduct, to post a copy of its apology in "a place that could be easily accessed by the public," to remove from its databases the negative information on the petitioner, and finally, to refrain from carrying out similar practices in the future. More info [here](#).

iii. Data transmission to security and intelligence agencies from providers of electronic communication services

CJEU: In the cases of *Privacy International, La Quadrature du Net and Others* (2020), the Court of Justice of the European Union (CJEU), in two related Grand Chamber judgments, held

that EU Law precluded national legislation requiring providers of electronic communications services to carry out general and indiscriminate transmission of traffic data and location data to security and intelligence agencies for the purpose of safeguarding national security. In joined applications by the United Kingdom, France and Belgium, the CJEU sought to determine the lawfulness of national legislation which laid down an obligation for providers of electronic communications services to forward users' traffic data and location data to a public authority, or to retain such data in a general or indiscriminate way on crime prevention and national security grounds. The Court found that such obligation not only interfered with the protection of privacy and personal data, but was also incompatible with the freedom of expression principle under Article 11 of the EU Charter. The Court, however, laid down that where such a retention is warranted in cases where there is a serious threat to national or public security, the nature of the measure must be "strictly" proportionate to its intended purpose. In addition, the Court also clarified the scope of powers conferred on Member States by the Privacy and Electronic Communications Directive with respect to retention of data for the aforementioned purposes. More info [here](#).

iv. Data protection and internet platforms

CJEU: In the case of *Data Protection Commissioner v. Facebook (Schrems II)* (2020), the Grand Chamber of the Court of Justice of the European Union (CJEU) invalidated the EU-US Privacy Shield and upheld the validity of the standard data protection clauses (an EU-approved standard contract to protect data transfers between EU and non-EU countries). In 2013, Schrems had brought a complaint before the Irish Data Protection Commission against Facebook Ireland Ltd. claiming mass surveillance of the data of EU citizens by US authorities. In a judgment delivered by CJEU in 2015, the Court invalidated the safe harbor privacy principles, subsequent to which Facebook used another legal tool to transfer data outside of the EU, called "standard contractual clauses" (SCCs). By an amended complaint dated December 1, 2015, Schrems challenged the validity of Facebook's use of SCCs to transfer EU citizens' data to the US, arguing that the use of such data for mass surveillance violated Art 7, 8 and 47 of the Charter of Fundamental Rights of the European Union (CFR). While declaring the EU-US Privacy Shield void for lack of 'adequate protection' under EU law, the Court held that CJEU's assessment of U.S. law must be taken into account for any transfers of personal data to the U.S., irrespective of the transfer mechanism used. Even though the validity of standard data protection clauses was upheld by CJEU, the Court noted that companies and regulators are required to conduct case-by-case analyses to determine whether foreign protections concerning government access to data transferred meet EU standards.

The Court noted that companies and regulators are required to conduct case-by-case analyses to determine whether foreign protections concerning government access to data transferred meet EU standards

In this decision the Court does not analyze the right to freedom of expression when considering the reasons for its ruling. Nonetheless, the scope of the protection of privacy in this particular case

provides a material protection of the right to freedom of expression against the chilling effect of surveillance or overly broad data collection. More info [here](#).

v. Requiring Internet Service Providers (ISPs) to store telecommunications data

CJEU: In the case of ***Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources (2014)***, the CJEU held that a European Union directive requiring Internet Service Providers (ISPs) to store telecommunications data in order to facilitate the prevention and prosecution of crime was found to be invalid under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Parallel cases were raised in Ireland and Austria following passage of the directive regarding the lawfulness of the measure. Each court forwarded the question to the CJEU where they were consolidated. The CJEU deemed the directive was legitimate in its aims of fighting serious crime but did not pass the proportionality test applied to evaluate the appropriateness of the measures undertaken to achieve the goal.

In this decision the Court does not analyze the right to freedom of expression when considering the reasons for its ruling. Nonetheless, the scope of the protection of privacy in this particular case provides a material protection of the right to freedom of expression against the chilling effect of surveillance or overly broad data collection. More info [here](#).

vi. National legislations establishing mass surveillance of electronic communications

CJEU: In the case of ***Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v. Watson (2017)***, the CJEU in a preliminary ruling held that national legislation establishing mass surveillance of electronic communications for the purpose of fighting crime violated the right to privacy and the right to data protection. The decision follows requests from UK and Swedish courts after the CJEU's earlier ruling in Digital Rights Ireland invalidating the EU's Directive 2006/24/EC on data retention on the grounds that a general obligation to retain certain communications data constituted a serious interference with the fundamental rights to respect for private life and to the protection of personal data, and that national rules affecting such obligation were not limited to what was strictly necessary for the purpose of fighting serious crime. The Court reasoned that the EU's Directive 2002/58 on privacy and electronic communications must be interpreted in light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFREU), namely the rights to privacy and data protection, and that national legislation which, for the purpose of fighting crime, provided for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication violated human rights law. The Court further reasoned that access of the competent national authorities to the retained data had to be restricted to fighting serious crime only, with prior review by a court or an independent administrative authority, and the data concerned had to be retained within the EU. More info [here](#).

Serbia: In the case of ***Serbia's Law on Electronic Communications (2013)***, the Constitutional Court of the Republic of Serbia found that the provisions of the Law on Electronic Communications, which dealt with data retention, were unconstitutional since they unjustifiably restrict the right to se-

crecy of correspondence and other means of communications prescribed in article 41 of the Constitution of Republic of Serbia. These provisions were declared to be unconstitutional because their formulation was not sufficiently precise and left open the possibility of accessing data without a court order.

In this decision the Court does not analyze the right to freedom of expression when considering the reasons for its ruling. Nonetheless, the scope of the protection of privacy in this particular case provides protection to the right to freedom of expression against the chilling effect of surveillance or overly broad data collection. More info [here](#)³.

vii. Electronic espionage: Pegasus spyware

India: In the case of *Manohar v. Union of India* (2021), the Supreme Court of India found that there was a *prima facie* case to create an Expert Committee to examine the allegations of unauthorized surveillance and privacy breaches by the Indian government and foreign parties on Indian citizens. Numerous petitioners, including journalists, lawyers and other human rights activists, alleged that their digital devices were compromised by Pegasus spyware, developed by an Israeli technology firm, on the basis of an investigation conducted by 17 media organizations from around the world. The Court ruled that unauthorized surveillance of stored data from the digital devices of citizens through spyware for reasons other than the nation's security would be illegal, objectionable, and could have far-reaching consequences to not only privacy rights, but also rights to freedom of expression. Given the government's refusal to provide information under the blanket defense of "national security", the Court found that it had failed to provide sufficient information to justify its position and thus ordered the creation of an independent committee to investigate the petitioners' allegations. More info [here](#).

viii. Interception of communications and access to phone records

United Kingdom: In the case of *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, et. al.*, (2016), *Specialized Court*, the UK Investigatory Powers Tribunal ruled that the obtaining by Security and Intelligence Agencies of Bulk Communications Data (BCD) from telecom operators was lawful under domestic law, namely Section 94 of the Telecommunications Act 1984, but that both the BCD and the Bulk Personal Datasets (BPD) regimes failed to comply with European Convention of Human Rights (ECHR) principles until their existence was made public. The campaign group, Privacy International, claimed that the acquisition and use of bulk personal and communications data by MI5, MI6 and Government Communications Headquarters (GCHQ) infringed the right to private life under Article 8 ECHR. The Foreign Secretary, the Home Secretary and the three security services argued that the use of these powers was lawful and essential for the protection of national security. The Court reasoned that the obtaining of BPD and BCD under rules and arrangements that were not publicly accessible fell foul of the ECHR

3 Previous to this ruling, the Constitutional Court of Serbia ruled on the constitutionality of other provisions of the Law on Electronic Communications in the cases of *Serb. Law on Military Security Agency and Military Intelligence Agency*, Articles 13.1, 16.2. (2012), Constitutional Court. More info [here](#); *Serb. Law on Telecommunications*, Article 55.1. (2009), Constitutional Court. More info [here](#).

Article 8 requirement that such measures must be “in accordance with law” because the rules were not sufficiently foreseeable or accessible and were not subject to adequate oversight.

In this decision the Court does not analyze the right to freedom of expression when considering the reasons for its ruling. Nonetheless, the scope of the protection of privacy in this particular case provides protection to the right to freedom of expression against the chilling effect of surveillance or overly broad data collection. More info [here](#).

South Africa: In the case of *amaBhungane Centre for Investigative Journalism v. Minister of Justice and Minister of Police (2021)* the South African Constitutional Court declared various elements of the legislation authorizing interception of communications unconstitutional and invalid. After a journalist learned that his communications had been intercepted, he and an investigative journalism center approached the Court, arguing that the legislation had serious shortcomings and infringed the right to privacy. The High Court held that the law was unconstitutional, and, on appeal, the Constitutional Court confirmed the High Court’s ruling. The Court emphasized that a lack of safeguards within the law prevented oversight and accountability, and the secrecy that covered the interception regime prevented any challenge to orders of surveillance. The Court noted that this secrecy and impunity heightened the risk of abuse and increased violations of the right to privacy. More info [here](#).

Zimbabwe: In the case of *Law Society of Zimbabwe v. Minister of Communications (2004)*, the Supreme Court of Zimbabwe struck down sections of the Postal and Telecommunications Act (the Act) that gave the President powers to intercept communications if he deemed it necessary in the interest of public safety. The Law Society of Zimbabwe had challenged the sections generally and, more specifically, in respect of communications covered by lawyer-client privilege. The Supreme Court found that sections 98(2) and 103 of the Act were too vague to adequately allow citizens to regulate their conduct and were thus too overreaching to be reasonably justified in a democratic society. Therefore, they did not satisfy the constitutional requirement of ‘provided by law’. Furthermore, as the Act did not provide any limitations or control mechanisms on the exercise of the President’s discretion, they unjustifiably infringed the right to freedom of expression and were unconstitutional. More info [here](#).

The Supreme Court of Costa Rica ruled it is a violation of freedom of expression and the confidentiality of sources to order a journalist’s phone records be released as part of an investigation into the possible commission of a crime by a third party.

Costa Rica: In the case of *Diario Extra v. Director of the Judicial Investigation Agency (2014)*, the Supreme Court of Costa Rica ruled it is a violation of freedom of expression and the confidentiality of sources to order a journalist’s phone records be released as part of an investigation into the possible commission of a crime by a third party. Representatives of the Costa Rican

newspaper *Diario Extra* filed a complaint that two investigative agencies obtained the phone records of a journalist at the newspaper in order to identify the person who was leaking confidential information to the journalist about criminal investigations. According to the Court, monitoring journalists' calls in the context of a criminal investigation against a third party not only violates the journalist's right to privacy, but also the right to confidentiality of sources, which is an essential condition for exercising the right to freedom of expression and information. For the phone records of a journalist to be legitimately monitored, the journalist must be under criminal investigation for committing a crime, and the monitoring warrant must be strictly proportionate to the objective pursued. The Court explained that for journalists, confidentiality of sources has a much broader scope of protection than other professions because such protection is essential for society to be properly informed and for journalists to properly fulfill their role. The Court ordered the elimination of all monitoring of incoming and outgoing phone calls made by or connected to the reporter, thus protecting the rights to privacy and the confidentiality of sources. More info [here](#).

Russia: In the case of *Telegram v. Federal Security Services* (2019), the Appellate Collegiate Body of the Supreme Court of Russia found that the Federal Security Services of Russia (FSS) had a lawful right to request that Telegram, a popular online messaging application, share with the FSS the keys needed to decrypt messages sent over its service. On April 14, 2017, the FSS sent a letter to Telegram's offices in London asking the company to provide it with keys to decrypt messages sent from six mobile numbers. Telegram received the letter but never shared the decryption keys. The FSS initiated a legal action against Telegram alleging that, by failing to satisfy the request, the company had violated the *Federal Law "On Information, Information Technologies, and Protection of Information"*. The first instance court fined Telegram RUB 800,000 (around \$13,000) for failing to comply with the FSS's requests. Telegram appealed to the appellate court, and the Supreme Court of Russia, arguing that the Russian courts had no jurisdiction to determine such a case against a UK-based entity, and that the request was unlawful since it was not made pursuant to a judicial order. Both upheld the law allowing the FSS to request that Telegram share the decryption keys. Telegram then appealed to the Appellate Collegiate Body of the Supreme Court of Russia, which, among other things, reasoned that the rights to privacy and secrecy in correspondence did not extend to the keys and, therefore, the FSS did not require a judicial order before it could request their disclosure.

This ruling illustrates the perils of the absence of independence of the judicial power. In this case, Russia's Supreme Court undermined the right to freedom of expression and privacy by upholding that a law enabled government authorities to request decryption keys from secure messaging mobile applications to access otherwise encrypted messages, without judicial oversight. This decision represents a direct attack against international human rights laws. More info [here](#).

ix. Surveillance of foreign telecommunications

Germany: In the case of *Reporters sans frontières and Others* (2020), the First Senate of the Federal Constitutional Court of Germany held that, under Article 1(3) of the Basic law, Grundgesetz – GG, German state authority is bound by the fundamental rights of the German constitution

when operating abroad. The Court found that foreign telecommunications surveillance conducted by the Federal Intelligence Service (Bundesnachrichtendienst – BND) violated the fundamental right to privacy of telecommunications, under Article 10(1) GG, and freedom of the press, under Article 5(1) GG. The appeal was brought by the Society for Civil Liberties (GFF) in coordination with Reporters Without Borders Germany (RSF), the German Journalists’ Association (DJV), German Journalists’ Union (DJU), the Network for Reporting on Eastern Europe (n-ost) and Netzwerk Recherche, along with several international investigative journalists in relation to alleged spying on journalists and their sources abroad. The constitutional complaint primarily challenged the 2016 amendment to the Federal Intelligence Service Act (Gesetz über den Bundesnachrichtendienst), which created a statutory basis for the telecommunications surveillance of non-German citizens in other countries. The judges reasoned that foreign intelligence gathering was not in theory incompatible with the constitution but needed to be justified, proportional and conducted with stricter oversight. Specifically, all data collection, processing and transfer to foreign entities under surveillance regimes must conform with constitutional obligations. The Court further recommended increased protections for those who could be endangered by transfers of such data, and for those “professional groups or groups of persons whose communications call for increased confidentiality,” such as lawyers and journalists. The challenged provisions continue to apply until 31 December 2021 to enable amendments to the statutory bases of telecommunications surveillance. More info [here](#).

x. COVID-19 Pandemic surveillance and data protection

Brazil: In the case of *Federal Council of the Brazilian Bar Association v. President Bolsonaro (2020)*, the Supreme Court stayed the implementation of a provisional measure which ordered telephone carriers to share all data of their subscribers with the Brazilian statistics agency. After the scheduled census moved from in-person to telephonic interviews, as a result of the COVID-19 pandemic, the Brazilian President enacted the measure, on the request of the statistics agency. The Brazilian Bar Association challenged this measure, arguing that it violated the constitutional protections of the right to privacy, the confidentiality of communications, and respect for private life. The Court held that there was a lack of protective measures and transparency in the measure and that its scope was too broad to justify the significant limitations to the rights to privacy and data protection. A number of the judges’ opinions in the case mentioned surveillance and abuse in data sharing as relevant concerns, underscoring the importance of personal data protection and the chilling effect surveillance has on freedom of expression. More info [here](#).

The Supreme Court of Israel held that the Israel Security Agency (“ISA”) is not constitutionally authorized to collect, process and use “technological information” of those who have tested positive for the coronavirus and their close contacts.

Israel: In the case of *Ben Meir v. Prime Minister (2020)*, the Supreme Court of Israel held that the Israel Security Agency (“ISA”) is not constitutionally authorized to collect, process and use “technological information” of those who have tested positive for the coronavirus and their close

contacts. The joint petitions were brought by the lawyer Shachar Ben Meir and rights organizations to challenge the Israeli Government’s decision (“the Enabling Decision”) to authorize the ISA to aid in coronavirus “contact tracing”. The Court found that section 7(b)(6) of the Israel Security Agency Law, 5762-2002 (“ISA Law”), which extends ISA jurisdiction to “essential national security interests of the State”, was too ambiguous to authorize such a significant expansion of the ISA’s activity over time without primary legislation. The Court further held that the Enabling Decision was a “serious violation of the right to privacy” [para. 36] and that, due to the fundamental importance of the freedom of the press, any contact tracing of journalists who tested positive for the coronavirus by the ISA would require their consent. While the Court appreciated the urgency of the public health crisis, it held that the “substantive flaws in the current mechanism” had to be replaced with a “transparent, voluntary mechanism.” The Court, therefore, recommended that Knesset Members implement primary legislation to continue the involvement of the ISA that is both provisional and a temporary order. More info [here](#).

India: In the case of *Balu Gopalakrishnan v. State of Kerala and Ors (2020)*, the High Court of Kerala issued an interim order directing the implementation of safeguarding measures to protect the confidentiality of data collected on patients or persons susceptible to COVID-19. A set of five petitions were filed in relation to a contract entered into by the Government of Kerala with Sprinklr Inc., a USA based software company, for creating an online data platform for data analysis of medical/ health data in relation to COVID-19. The petitions claimed that the contract lacked any safeguard against the unauthorized exploitation of health data collected by Sprinklr, on behalf of the State of Kerala. The Court stressed the urgency under the current circumstances to protect the confidentiality of personal data in order to avoid a “data epidemic.” In light of those concerns, the Court directed the State to anonymize all the sensitive personal data thus far collected with respect to COVID-19 before transferring it to Sprinklr, or any third-party service provider. Further, any future collection of data must be based on principles of informed consent where every individual will be informed about the access of such data by third parties. The Court also prohibited Sprinklr from committing any act in breach of confidentiality of the data and directed Sprinklr to entrust all the residual COVID-19 related data back to the State government.

In this decision the Court does not analyze the right to freedom of expression when considering the reasons for its ruling. Nonetheless, the scope of the protection of privacy in this particular case provides protection to the right to freedom of expression against the chilling effect of surveillance or overly broad data collection. More info [here](#).

xi. Surveillance and tracking by private actors⁴

Peru: In the case of *Acuña v. Minera Yanacocha SRL (2020)* the Constitutional Court of

4 The following Courts have also analyzed the impact of surveillance and tracking by private actors can have on freedom of expression and privacy: [Belgium](#): Nederlandstalige rechtbank van eerste aanleg Brussel, 2015/57/C (2015), First Instance Court; More info [here](#). [United States](#): The case of Google Inc. Cookie Placement Consumer Privacy Litigation (2015), Appellate Court, More info [here](#).

Peru held that the continuous use of surveillance technologies, by private corporations, entails a violation of privacy rights. The application was brought by a local environmental activist against a mining company for the use of surveillance cameras and drones that recorded and took pictures of her home. The Court stressed that the use of these devices was not unconstitutional *per se*, but only when they were employed in unreasonable or disproportionate manners. The Court held that the permanent use of the video camera and the possibility of constant overflight on the residence of the plaintiff constituted a constraint on her freedoms and privacy.

In this decision the Court does not analyze the right to freedom of expression when considering the reasons for its ruling. Nonetheless, the scope of the protection of privacy in this particular case provides a protection of the right to freedom of expression against the chilling effect of surveillance or overly broad data collection. More info [here](#).

xii. Anonymity⁵

ECtHR: In the case of *Standard Verlagsgesellschaft mbH v. Austria (No. 3) (2021)*, the Fourth Section of the ECtHR unanimously ruled that requiring the applicant to disclose personal information of its registered users violated the applicant's freedom of expression. The applicant was a media company, publisher of the offline newspaper and its online version *Der Standard*. The case concerned online comments published by registered users on the applicant's website against two right-wing Austrian politicians. The politicians and the political party requested the applicant to remove the comments and disclose the identities of the two authors to initiate civil and criminal procedures. The applicant deleted the comments but refused to provide the identity of the authors. On an application by the political leaders, the Supreme Court of Austria ordered the applicant to disclose personal data of the users. The Court found this to be a violation of the applicant's Article 10 rights. By not taking into account the political nature of the contested comments and by not running any test on balancing competing interests, the domestic courts failed to protect the applicant's right to freedom of expression. More info [here](#).

xiii. Publication of personal data by public agencies

India: In the case of *Saket v. Union of India (2020)*, the High Court of Bombay held that the Ministry of Information and Broadcasting should not have uploaded the personal details of the applicant to its government website following his lodging of an information request under the Right to Information Act, 2005. In this case, the applicant's personal data (including his name, home address, email address and telephone/mobile number) had been uploaded onto the Indian government website, which caused him immense trauma and public harassment. The Court found that the Ministry's decision to upload his personal details was unnecessary and made the applicant

⁵ In the Case of Doe v. Harris (2014), the United States Court of Appeals for the Ninth Circuit also analyzed how the protection of anonymity reinforces freedom of expression and privacy by granting the Plaintiffs a preliminary injunction blocking the enforcement of provisions which required anyone who is a registered sex offender to turn over a list of all their Internet identifiers and service providers to law enforcement. More [here](#).

vulnerable to intimidation and other harassment by the public. Further, the Court held that such disclosure of confidential data was not only a clear breach of the applicant’s privacy, but also defeated the purpose of the Right to Information Act, 2005 by deterring future applicants from filing applications due to fear of public disclosure of sensitive information. More info [here](#).

In the case of *Banners Placed on Roadside in the City of Lucknow v. State of Uttar Pradesh (2020)*, the Allahabad High Court ruled that the posting of banners by State officials publicizing personal details of individuals accused of vandalism was a violation of the fundamental right to privacy. The Chief Justice of the Allahabad High Court invoked its public interest jurisdiction and initiated *suo moto* proceedings against the Lucknow District administration and the Police administration (State Executive) for posting the large-scale banners at major roadside areas in response to damage done during a protest against the Citizenship Amendment Act in December 2019. The Court held that the displaying of photographs, names and addresses of certain persons publicly by the State Executive was an “unwarranted interference with [their] privacy.” Publication of such personal details by the State failed to satisfy the three-part test of legality, legitimacy and proportionality. Accordingly, the Court directed the State to take down the banners and prohibited the public placement of any additional banners containing personal data of individuals without authority of law. More info [here](#).

The disproportionate measures used to enforce the Act, the lack of necessary and a legitimate purpose, and absence of safeguards against misuse of the data collected under the Act were the primary grounds on which the Court declared the Act to be unconstitutional.

xiv. Compulsory registration in databases⁶

Jamaica: In the case of *Robinson v. Attorney General (2019)*, a three-judge bench of the Supreme Court of Judicature of Jamaica held the National Identification and Registration Act (“NIRA” or the “Act”), in its entirety, to be unconstitutional on the grounds of violating the right to privacy and equality. The Act required Jamaican citizens and residents of more than six months to mandatorily enroll in the database and provide biographic and core biometric data. To ensure enforcement of the Act, criminal sanctions were provided for individuals who failed to enroll themselves. The Court, while giving an extensive interpretation of the right to privacy held the mandatory nature of the Act and the criminal sanctions to be in violation of informational privacy and liberty of the individuals. The disproportionate measures used to enforce the Act, the lack of necessary and a legitimate purpose, and absence of safeguards against misuse of the data collected under the Act were the primary grounds on which the Court declared the Act to be unconstitutional.

In this decision the Court does not analyze the right to freedom of expression when considering

⁶ Decisions regarding registration in COVID-related databases can be found on section x. *COVID-19 Pandemic surveillance and data protection*.

the reasons for its ruling. Nonetheless, the scope of the protection of privacy in this particular case provides protection to the right to freedom of expression against the chilling effect of surveillance or overly broad data collection. More info [here](#).

India: In the case of *Puttaswamy v. Union of India (I) (2017) / 2017 (10) SCALE 1*, a nine-judge bench of the Supreme Court of India held unanimously that the right to privacy was a constitutionally protected right in India, as well as being incidental to other freedoms guaranteed by the Indian Constitution. The case, brought by retired High Court Judge Puttaswamy, challenged the Government's proposed scheme for a uniform biometrics-based identity card which would be mandatory for access to government services and benefits. The Government argued that the Constitution did not grant specific protection for the right to privacy. The Court reasoned that privacy is an incident of fundamental freedom or liberty guaranteed under Article 21 which provides that: "No person shall be deprived of his life or personal liberty except according to procedure established by law". This is a landmark case which is likely to lead to constitutional challenges to a wide range of Indian legislation, for example legislation criminalising same-sex relationships as well as bans on beef and alcohol consumption in many Indian States. Observers also expect the Indian Government to establish a data protection regime to protect the privacy of the individual. Further, the case is likely to be of wider significance as privacy campaigners use it to pursue the constitutional debate over privacy in other countries. More info [here](#).

xv. Facial recognition

Brazil: In the *Case of São Paulo Subway Facial Recognition Cameras (2021)*, a civil court in São Paulo held that the use of facial recognition technology on a subway line was an infringement of the right to privacy of one's image. After the operator of a subway line in São Paulo introduced interactive subway car doors which displayed personalized advertisements to the passengers based on information gathered through facial detection technology, a consumer rights organization approached the Court seeking damages and an order prohibiting the use of the equipment. The Court held that the use of any facial recognition or detection software required the consent of users and ordered the subway operator to cease using the technology.

In this decision the Court does not analyze the right to freedom of expression when considering the reasons for its ruling. Nonetheless, the scope of the protection of privacy in this particular case provides a material protection of the right to freedom of expression against the chilling effect of surveillance or overly broad data collection. More info [here](#).

United States: In the case of *Patel v. Facebook (2019)*, the United States Court of Appeals for the Ninth Circuit held that facial-recognition technology used to create face templates without prior consent invades individuals' interests and privacy. In 2010, Facebook started using facial-recognition technology to develop its Tag Suggestions feature without the users' prior written consent and without a retention schedule of the biometric information. Three Facebook users in Illinois filed a complaint in 2015, alleging that Facebook's facial-recognition technology violated the Illinois Biometric Information Privacy Act. The Court affirmed the decision of the United States

District Court for the Northern District of California, confirming that Facebook’s facial-recognition technology affected users’ privacy and personal affairs, and noted the impact technological advances may have on privacy.

In this decision the Court does not analyze the right to freedom of expression when considering the reasons for its ruling. Nonetheless, the scope of the protection of privacy in this particular case provides a material protection of the right to freedom of expression against the chilling effect of surveillance or overly broad data collection. More info [here](#).

xvi. Access to the internet, privacy, and freedom of expression

India: In the case of *Shirin R.K. v. State of Kerala* (2019), the High Court of Kerala held that a restriction imposed on the use of mobile phones in a women’s hostel was an unreasonable infringement upon the right to access the internet, the right to privacy, and the right to education. Fareema Shirin, a student, brought the challenge after being ordered to vacate college housing for refusing to comply with a rule restricting mobile phone usage during designated hours. The Court relied on international conventions to find that the hostel had an obligation to ensure women’s on-line freedom of expression and that digital resources offer important opportunities for affordable and inclusive education necessary to advance students’ careers. The Court ordered the College to modernize the policies so they do not discriminate based on gender or undermine students’ access to educational resources. Finding the restriction to be “absolutely unwarranted,” the Court further ordered Shirin’s immediate re-admission to the hostel and declared that the right to access the Internet has become part of the right to education as well as the right to privacy under Article 21 of the Constitution of India. More info [here](#).

xvii. Personal correspondence

ECtHR: In the case of *Bosyy v. Ukraine* (2018), the Fifth Section of the ECtHR found that a Ukrainian law allowing the automatic monitoring and censorship by the prison authorities of a prisoner’s correspondence was a violation of the prisoner’s right to privacy. Bosyy spent seven years in prison during which time he alleged his correspondence was regularly “intercepted, reviewed, blocked or delayed,” which negatively impacted his communications with the Court and other bodies regarding his case. Citing its previous case law, the Court concluded that the amended national laws did not provide appropriate protection against arbitrary interference, that they were “defective” and therefore, the existing monitoring regime was not in “accordance with the law.” As a result, there was a violation of privacy rights protected under article 8 of the ECHR.

In this decision the Court does not analyze the right to freedom of expression when considering the reasons for its ruling. Nonetheless, the scope of the protection of privacy in this particular case provides protection to the right to freedom of expression against the chilling effect of surveillance or overly broad data collection. More info [here](#).

xviii. Protection of journalistic sources

ECtHR: In the case of *Nagla v. Latvia* (2013), the Fourth Section of the European Court

of Human Rights (ECtHR) held that Latvian investigating authorities had failed to protect the sources of a journalist and thus violated Article 10 of the European Convention on Human Rights (ECHR). After news program host Ilze Nagla had gone on air to inform the public of an information leak from the State Revenue Service database, the investigating authorities searched her home and seized several data storage devices. While the Court recognized the importance of securing evidence in criminal proceedings, it stressed that “a chilling effect” could arise when journalists were expected to assist in the identification of anonymous sources. The Court held that a search conducted with the aim of identifying a journalist’s source was a measure more extreme than an order to disclose the source’s identity. More info [here](#).

B. Balancing the competing rights of privacy and freedom of expression

In the following pages we have systematized cases from different jurisdictions in which freedom of expression and privacy come into tension. Cases are ordered by topic, country, and court of origin. In most cases, the paper does not explain the criteria used by judges to solve them, since the document only systematizes the summaries of the cases in our database that were prepared by [researchers](#) and [experts](#) affiliated with our program. For this reason, at the end of each case summary we have included a link to the database entry of the case, in which it is possible to find a more detailed description of the ruling.

The criteria we have used to classify the cases stem from that used by courts to balance competing rights, by virtue of the harmonization principle. As announced in the introduction, the number of cases in which there are tensions between the right to privacy and freedom of expression is enormous. In some cases, tribunals with robust and respectable traditions have arrived at different conclusions. However, in all the emblematic cases, courts have taken into account two criteria: the public interest of the information — either because it concerns information about a public official, a public figure, or information relevant to the public opinion— and the degree to which privacy is affected. This last criterion refers to the source of the information, how it was obtained and to the content of the information itself. We tried to follow these criteria to identify the cases selected in this small sample.

The European Court of Human Rights (ECtHR) held that the publication by tabloid magazines of a series of photos of Princess Caroline of Monaco, taken without her knowledge and showing scenes from her daily life, violated her right to privacy and family life as enshrined in Article 8 of the European Convention on Human Rights (ECHR).

i. Public figures, privacy and public interest

ECtHR: In the case of *Von Hannover v. Germany (No. 1)* (2004), the European Court of Human Rights (ECtHR) held that the publication by tabloid magazines of a series of photos of Princess Caroline of Monaco, taken without her knowledge and showing scenes from her daily life,

violated her right to privacy and family life as enshrined in Article 8 of the European Convention on Human Rights (ECHR). The Court was presented with a conflict between the freedom of the press and the right to protect private life, particularly of public figures. The Court rejected the German Courts' decisions, which had found that the applicant was undeniably a contemporary public figure par excellence and thus, had to tolerate the publication of such photographs even when they were not related to her official duties. The Court held that the press reporting details about the applicant's personal life, notably as she did not exercise an official State function, did not fall under the watchdog role of the press and did not contribute to a debate of general interest. More info [here](#).

In the case of *Von Hannover v. Germany (No. 2)* (2012), the Grand Chamber of the ECtHR found that two photographs depicting a royal family on holiday and published in two German newspapers violated the right to privacy pursuant to Article 8 of the ECHR because they did not reflect any matter of public interest detailed in the accompanying text. However, a third photograph depicted a Prince in poor health, and since the health of the Prince was a matter of public concern, the ECtHR found no violation of Article 8. In reaching its ruling, the ECtHR set out the criteria which domestic courts should follow when balancing the right to privacy pursuant to Article 8 against the right to freedom of expression under Article 10. Firstly, whether the information contributes to a debate of general interest; second, how well known is the person concerned and the subject matter of the report; thirdly, the prior conduct of the person concerned; fourthly, content, form and consequences of the publication; and fifth, the circumstances in which the photos were taken. More info [here](#).

In the case of *Axel Springer AG v. Germany* (2012), the Grand Chamber of the ECtHR ruled by 12 votes to five that Germany had violated the applicant's right to freedom of expression when it fined a magazine and prohibited further publication of articles concerning the arrest of an actor for cocaine possession. The actor had brought an action alleging that the magazine had breached his right to privacy. The Court reasoned that the articles concerned public judicial facts obtained from official sources about someone well-known to the public regarding an arrest in a public place, albeit for a minor and common crime and that, although the sanctions were lenient, they were unnecessary in a democratic society and disproportionate to the legitimate aim pursued. The Court also set forth six criteria to take into consideration when balancing freedom of expression and the right to privacy: (1) the contribution to a debate of general interest, (2) the subject of the report and that it concerned a public figure, (3) the prior conduct of the person concerned, (4) the method of obtaining the information and its veracity, (5) the content, form, and consequences of the media content, and (6) the severity of the sanction imposed. The dissenting Judges agreed with the majority's assessment of the facts, but they felt that the majority had simply reached a different conclusion giving more weight to freedom of expression than privacy in comparison to the domestic courts, and hence gone beyond the Court's remit as it was not supposed "to repeat anew assessments duly performed by the domestic courts". More info [here](#).

In the case of *Lillo-Stenberg v. Norway* (2014), the First Section of the ECtHR found Article 10 of the ECHR protected the right of a Norwegian magazine to publish an article containing

photos and descriptions of a celebrity couple's private wedding; there was no violation concerning the couple's right to privacy under Article 8 of the ECHR. Even though the wedding was a private event, the fact that weddings have a public component and that no deliberately private facts were unlawfully made public, tipped the balance away from the couple's Article 8 right and in favor of the magazine's Article 10 right to freedom of expression. More info [here](#).

In the case of *MGN Limited v. United Kingdom* (2011), the Fourth Section of the ECtHR found that a restriction on the publication of private information did not violate the publisher's Article 10 rights. However, excessive success fees as costs for liability were a violation of Article 10. The applicant was the publisher of UK's national daily newspaper, the Daily Mirror. The paper published several articles regarding Ms. Naomi Campbell's drug addiction. The articles provided details of the addiction and treatment, and two photographs of Ms. Campbell waiting outside the place of treatment. In a 6:1 decision, the Court found that disclosing that Ms. Campbell was a drug addict in treatment was in the public interest because Ms. Campbell had previously publicly denied drug use. However, additional details of her method of treatment and the two photographs were not in public interest and violated Ms. Campbell's right to privacy. As part of a conditional fee agreement, the applicant was required to pay 95% and 100% of the costs in the House of Lords as success fees to the solicitors involved. The Court held that the success fees were a disproportionate interference with the applicant's right to free speech because it could have a chilling effect on media organizations, discouraging them from publishing legitimate information and encouraging them to settle claims instead of defending them. More info [here](#).

The novel, titled *Mephisto*, tells the fictional story of Hendrik Höfgen, a talented actor who colludes with the Nazi powers to advance his career [...] Gründgens' adoptive son, Peter Gorski, brought proceedings against the publishing house Nymphenburger Verlagshandlung, seeking to prevent the publication of *Mephisto* in West Germany.

In the case of *Ricci v. Italy* (2013), the Second Section of the ECtHR considered that Italy violated Article 10 of the ECHR when it upheld a television producer's conviction for showing images from an illicitly taped video interview featuring philosopher Gianni Vattimo. The court acknowledged the producer's conduct was prescribed by Italian law, and legitimately justified under Article 10(2) of the ECHR, but held that the punishment – a €30,000 fine and a four-month term of imprisonment – was disproportionate to the producer's conduct. More info [here](#).

Germany: In *The Case of Mephisto* (1971), the Federal Constitutional Court of Germany upheld a lower court decision granting an injunction that banned a novel from being published in West Germany. The novel, titled *Mephisto*, tells the fictional story of Hendrik Höfgen, a talented actor who colludes with the Nazi powers to advance his career. The titular character of the novel

was based on real-life actor Gustaf Gründgens. In 1963, Gründgens' adoptive son, Peter Gorski, brought proceedings against the publishing house Nymphenburger Verlagshandlung, seeking to prevent the publication of *Mephisto* in West Germany. The Federal Constitutional Court of Germany considered that although artistic freedom is protected by the German Constitution, in this case, lower courts were right to invoke the right to dignity, as laid out in the Constitution, to protect the personality rights of Gründgens, thus upholding a ban on the publication of the novel. More info [here](#).

United States: In the case of *Sidis v. F-R Pub. Corp. (1940)*, the U.S. Court of Appeals for the Second Circuit held that a magazine article about a once-famous prodigy did not violate his privacy. William James Sidis, who had gained fame as a child and teenager but pursued a more ordinary life as an adult, initiated the proceedings, alleging that *The New Yorker* magazine had unveiled details about his current life and thus violated his right to privacy. The Court reasoned that scrutiny about Sidis's life could be of public concern, and was hence justified due to his earlier publicity. The Court also held that no illegal use of Sidis's name, picture, and portrait for trade or advertisement purposes had occurred. More info [here](#).

ii. The duty to notify subjects before publishing articles concerning their private life

ECtHR: In the case of *Mosley v. The United Kingdom (2011)*, the Fourth Section of the ECtHR concluded that the United Kingdom had not failed its positive obligations in relation to the right to privacy. The complaint had been brought by an individual who had recovered monetary compensation from the domestic courts for having had his privacy infringed by a newspaper article concerning sexual activities in which he had engaged in private. The complainant maintained that, in order to adequately protect privacy, the UK had a duty to require publishers to notify subjects before the publishing of articles concerning their private life, in order to afford them the opportunity to request an injunction before publication. The Court reasoned that, in light of its potential “chilling effect” on freedom of expression, its questionable effectiveness and the wide margin of appreciation afforded to individual Members, States could not be said to have an obligation to impose such a pre-notification requirement. More info [here](#).

The complaint had been brought by an individual who had recovered monetary compensation from the domestic courts for having had his privacy infringed by a newspaper article concerning sexual activities in which he had engaged in private.

In the case of *Peck v. The United Kingdom (2003)*, the European Court of Human Rights found that the United Kingdom violated the right to privacy, as enshrined in Article 8 of the European Convention on Human Rights, of the applicant, when the Brentwood Borough Council disclosed footage, —to several media outlets— recorded by its CCTV system, of the applicant's suicide attempt, in a public street, and its aftermath. For the ECtHR, the United Kingdom failed to take the necessary safeguards to protect the privacy of the applicant, such as masking the identity

of the applicant in the disclosed footage or obtaining the applicant's consent to release the footage. Thus, the Court considered that although the disclosure of the footage was provided by law and pursued a legitimate aim, it was an unnecessary and disproportionate' interference with the applicant's right to privacy. More info [here](#).

iii. Publication of private information of public interest available on the public dominion

ECtHR: In the case of *Flinkkilä v. Finland* (2010), the European Court of Human Rights (ECtHR) found that the State of Finland violated Article 10 of the European Convention when its national courts ordered the editors and journalists of two magazines to pay fines and damages, in the context of criminal proceedings, for publishing news articles mentioning the name and identity of B, the female friend of the National Conciliator, and their involvement in a violent altercation. The national courts considered that these articles were an unjustified invasion of B's privacy. For the ECtHR, the interference on the freedom of expression of the claimant, although it was prescribed by law and pursued a legitimate aim, was disproportionate and thus not necessary in a democratic society, since B's identity had been previously disclosed on national television, the questioned news articles were of public interest, and the sanctions too severe. More info [here](#).

iv. Publication of private photos from social media not directly related to matters of public interest

Spain: In the case of *Dario v. La Opinión de Zamora* (2020), the Spanish Constitutional Court confirmed the Supreme Court's award of damages to a man whose social media photographs had been published by a Spanish newspaper. The man had sued the newspaper after a report on his brother's suicide had included photographs from the man's private Facebook account. The Constitutional Court recognized that there is a balance to be found between a newspaper's right to freedom of expression and an individual's right to privacy, and held that the publication of private photographs which were not directly related to a matter of public interest was an infringement of the right to privacy. The Court stated that the mere sharing of images on social media by an individual does not authorize the use of those images by third parties without the individual's consent. More info [here](#).

v. Radio broadcast of a private conversation of public interest

ECtHR: In the case of *Radio Twist v. Slovakia* (2006), the European Court of Human Rights held that a recording about a public figure, and relating to matters in the public interest, outweighed an individual's right to privacy even though the recording was illegally obtained and presented in a format that was not clearly audible. The domestic courts' order that the applicant broadcasting company deliver a written and broadcast apology and pay a fine was an unjustified interference with its right to impart information under Article 10(1). The European Court reiterated the essential role the press fulfills in a democratic society and that the restrictions on its freedom of expression must be construed strictly. More info [here](#).

United States: In the case of *Bartnicki v. Vopper* (2001), the U.S. Supreme Court of the United States absolved a radio station of liability for broadcasting a conversation between two union

representatives that was recorded by a third party. The two union representatives sued a radio commentator who played a tape of a recorded conversation they had in the midst of collective bargaining negotiations. The radio station claimed that the disclosure of the conversation over the radio was protected under the First Amendment's freedom of speech. The Court reasoned that the First Amendment protects a rebroadcast on the radio because the conversation was a matter of public concern and the radio station did nothing illegal to obtain the tape. More info [here](#).

vi. Publication of health-related information about public officials

ECtHR: In the case of *Éditions Plon v. France* (2014), the European Court of Human Rights (ECtHR) found that France violated Article 10 of the European Convention of Human Rights when its domestic courts banned indefinitely the book *Le Grand Secret* published by Éditions Plon. The book was co-authored by Dr. Gubler, a private physician to then President François Mitterrand, and gave a detailed account of the President's illness, and subsequent treatment. The book was published shortly after the death of Mitterrand. Upon request from Mitterrand's heirs, national French Courts banned the book indefinitely arguing that it breached medical confidentiality. For the ECtHR, an indefinite ban on the book was a disproportionate measure not necessary in a democratic society. More info [here](#).

In the case of *Fürst-Pfeifer v. Austria* (2016), the Fourth Section of the ECtHR held that a psychiatrist's privacy rights had not been violated when her mental health information was published in an article online and in print. The article mentioned that she had suffered from mental problems while working as a court-appointed expert. The European Court of Human Rights declared that the health status of a physiological expert is a debate of general interest. Further, the Court held that court-appointed civil servants are subject to wider criticism than ordinary citizens. Dissenting judges argued that the majority failed to balance competing privacy and freedom of expression rights, as their analysis focuses solely on freedom of expression guaranteed by Article 10 of the European Convention on Human Rights. More info [here](#).

Argentina: In the case of *Ponzetti de Balbín v. Editorial Atlantida S.A.* (1984), the Supreme Court of Argentina held that the publication of photographs by a magazine of a renowned political figure violated his right to private life. Renowned politician Ricardo Balbín's son brought a lawsuit against the publisher and owner of the magazine, *Gente y la actualidad*, after it published an issue featuring on its cover a photograph of Balbín that was taken while he lay on his deathbed in a hospital. The Court explained that even public figures have the right to keep certain aspects of their lives private, and that publishing these photographs did not serve the public, because the news of Balbín's death could have been provided to the public without them. More info [here](#).

vii. Publications about people with HIV

ECtHR: In the case of *Armoniene v. Lithuania* (2008), the Second Section of the ECtHR held that protection of the right to privacy as entrenched in Article 8 of the ECHR extended beyond the private family circle to include a social dimension. In 2002, a major Lithuanian newspaper disclosed that Ms. Armonienė's husband was HIV positive and that he had two children with another woman who also had the disease. Lithuanian courts awarded him the maximum sum for non-pe-

cuniary damage. However, after Ms. Armonienė’s husband passed away, she appealed the national court’s decision arguing that the adjudged sum of money was inappropriate and there was a violation of her husband’s right to an effective domestic remedy for the infringement of her right to privacy. The ECtHR determined that protecting the confidentiality of a person’s HIV status was especially important since disclosure of that information could lead to humiliation and the risk of ostracism. Furthermore, the ECtHR noted that such disclosure could dissuade people from undertaking voluntary HIV tests. Regarding the publication of Ms. Armonienė’s HIV status, the Court held no public interest in disseminating such information. Instead, it found that the sole purpose of the publication was apparently to satisfy the readership’s curiosity. The Court concluded that in such cases of an “outrageous abuse of press freedom,” the severe legislative limitations on judicial discretion in redressing the damage suffered by the victim and thus on deterring the recurrence of such abuses had failed to provide Ms. Armonienė with the protection of privacy she could have legitimately expected. As a result, the Court determined that Ms. Armonienė suffered non-pecuniary damages that had not been sufficiently compensated and awarded her the sum of 6,500 euros, 3,604 euros more than the maximum sum allowed in such circumstances under Lithuanian legislation. More info [here](#).

The Constitutional Court of South Africa ruled that the disclosure of private and confidential medical information in a book without the full and informed consent from the individuals was an infringement of their right to privacy

South Africa: In the case of *NM v. Smith* (2007), the Constitutional Court of South Africa ruled that the disclosure of private and confidential medical information in a book without the full and informed consent from the individuals was an infringement of their right to privacy. Three women living with HIV who had participated in an HIV clinical drug trial and whose names had been published in an official academic report related to the trials learned that their names and HIV status had been published in a biography about a politician without their consent. The women approached the High Court, arguing that this publication infringed their rights to privacy, dignity, and psychological integrity. The High Court held that there had been no infringement of the rights and the Supreme Court of Appeal declined to hear their appeal. The Constitutional Court found that there was no need to develop the common law around privacy violations to include liability for negligence as the author of the book had acted with sufficient intention in publishing the women’s private facts as she had not taken the necessary steps to determine whether the women had consented to their identities being made public. The minority judgment stressed the need to balance the rights to privacy and to freedom of expression and would have held that the common law should be developed, and that – given her position as a member of the media – the author had acted reasonably in relying on information provided in an official academic report. More info [here](#).

viii. Information about patients in psychiatric hospitals

United Kingdom: In the case of *R v. Secretary of State for Justice* (2016), the UK Supreme

Court reversed the lower court's decision and granted an anonymity order to a British national who was compulsorily admitted in a psychiatric hospital and had had his request for unescorted community leave turned down by the UK Secretary of State. The patient had applied for judicial review before the High Court and the hospital's clinician responsible for the patient had requested the court to issue an anonymity order. The Court ordered the identity of the hospital and its staff to remain anonymous, but it refused to conceal the patient's identity on the ground that his previous proceedings were publicly available. The UK Supreme Court held that whether an anonymity order related to legal proceedings of a mental patient is necessary must be assessed on a case-by-case basis. Yet "[t]he public's right to know has to be balanced against the potential harm, not only to this patient, but to all the others whose treatment could be affected by the risk of exposure." (*R. v. Secretary of State*, [2016] UKSC 2, para. 36.) With respect to the patient in the present case, the Supreme Court reversed the lower court's decision, finding it necessary to preserve his identity as well. The Court was of the opinion that the disclosure of his identity could jeopardize his treatment and re-integration into the community. More info [here](#).

ix. Publication of images of a public official

ECtHR: In the case of *Alpha Doryforiki v. Greece* (2018), the Grand Chamber of the ECtHR found that the Greek Courts had violated the applicant TV broadcaster's freedom of expression by imposing sanctions on the applicant for the broadcast of a secretly filmed video of a public official in a public place. However, the Court held that there had been no violation in respect of two further videos that had been secretly filmed on private premises. The videos showed, respectively, a parliamentary deputy who was also chairman of the inter-party committee on electronic gambling, entering a gambling arcade and playing on two machines; a meeting between the deputy and associates of the television host during which the first video was shown to the deputy; and a meeting between the deputy and the host in the latter's office. The Greek Supreme court upheld the decision of the National Radio and Television Council which had fined the applicant 200,000 euros and ordered it to broadcast the Council's full decision on its main news. The ECtHR reasoned that in balancing the competing rights of privacy, Article 8, and freedom of expression, Article 10, the Greek courts had not taken into account the fact that the first video was not recorded on private premises and that the interference with the official's privacy rights under Article 8 was therefore significantly less serious than the interference occasioned by the second two videos, where the Greek courts had struck a fair balance between the competing rights taking into account the way the information was obtained, and the journalistic duties and obligations of the applicant company. More info [here](#).

Germany: In the case of *Wowereit v. Axel Springer SE* (2016), the Supreme Court of Appeal in Germany (Bundesgerichtshof) overruled the lower courts' finding that a newspaper had violated the personality rights of the Mayor of Berlin by publishing photographs of him having drinks on the eve of a significant parliamentary vote on his competence. The Supreme Court of Appeal found that the publisher of the German newspaper *BILD-Zeitung*, which is part of the publishing house Axel Springer SE, was justified in publishing the photographs as they were published in the context of a political event and, therefore, contributed to a story of public interest. In reaching this conclusion, the Supreme Court of Appeal reasoned that the photograph provided the public with

information about his behavior on the night before a vote that could decide the future of his political career, and could then help inform public opinion on his character. More info [here](#).

x. Private images or information of no public interest

ECtHR: In the case of *Ruusunen v. Finland (2014)*, the Fourth Section of the ECtHR found that the publication of details regarding the private sex life of Finland's Prime Minister, published in a book written by his ex-girlfriend, breached the Prime Minister's right to privacy. More info [here](#).

Ecuador: In the case of *Nonconsensual Pornography sent to Victim's Parents (2021)*, the Constitutional Court of Ecuador held that the storage and sharing of sexual photos without the consent of the victim were a violation of her constitutional rights to personal data protection, reputation, and intimacy. The victim pursued a habeas data action against the defendant, who had found the pictures in a family-shared computer, saved them in flash memory, and sent them to the parents of the victim. The Court reasoned those intimate images were personal data sent exclusively to the defendant's partner and required previous consent to be processed by anyone else. When the defendant saved the photos and shared them with other people, she inflicted damage and violated human rights grounded on dignity and informational self-determination. More info [here](#).

The Inter-American Court of Human Rights considered that a series of publications about the unrecognized son of the then president of Argentina Carlos Saul Menem with a congresswoman, Menem's relationship with the congresswoman, and the relationship between the president with his son, were of public interest.

Kazakhstan: In the case of *WA and WB v. Mamedov (2019)*, the Supreme Court of Kazakhstan upheld fines against a man who recorded and published a video on Facebook of two women without their consent, and by doing so exposed their sexual orientation. WA and WB were secretly recorded kissing by a stranger at a cinema. The stranger then posted the video on Facebook, criticizing their sexual preferences and called on the women to be outed and shamed. The video became viral in Kazakhstan and led to the women becoming targets of harassment and threats. The two were forced to flee Kazakhstan for several months, and eventually sued the man for violating their privacy, and sought compensation for moral harm. The first instance court ruled for the women, only for the judgment to be overturned by an appellate court on the ground that the women's behavior was amoral. The Supreme Court reinstated the first instance judgment, reiterating that the man violated the women's right to privacy by recording them without their consent, publishing the subsequent video on social media, which in turn caused the women great harm. More info [here](#).

Canada: In the case of *R. v. Jarvis (2019)*, the Supreme Court of Canada convicted a teacher for voyeurism for secretly recording his students in common areas of a school. This offence is committed when a person secretly observes or makes a visual recording of another person with a sexual

purpose where the person being observed or recorded has a reasonable expectation of privacy. The Court concluded that the teacher acted contrary to the reasonable expectations of privacy when he recorded the students' breasts, faces and upper bodies with a pen camera while they engaged in school activities. The Court held that people do have a reasonable expectation of privacy in public spaces, such as school grounds, and that where a person "does not expect complete privacy [this] does not mean that she waives all reasonable expectations of privacy" [para. 61]. More info [here](#).

xi. Publications about a public official's family life

IACtHR: In the case of *Fontevicchia and D'amico v. Argentina* (2011), the Inter-American Court of Human Rights considered that a series of publications about the unrecognized son of the then president of Argentina Carlos Saul Menem with a congresswoman, Menem's relationship with the congresswoman, and the relationship between the president with his son, were of public interest. As a result, the Inter-American Court considered that the subsequent imposition of liability on the editor and director of the paper that published the information did not meet the necessary requirements and infringed the right to freedom of expression. More info [here](#).

xii. Publications regarding accusations against public officials for sexual offenses

Mexico: In the case *Municipal President of Acambaro v. General Director of the Newspaper "La Antorcha"* (2009), the Supreme Court of Mexico reversed a lower court decision that imposed a criminal conviction against the general director of a newspaper who published an interview that contained allegations made by a former public official regarding several acts of corruption carried out by the municipal president. Additionally, the interviewee mentioned a possible act of sexual harassment, attributable to the municipal president, in the following terms: "one day, at the hotel in the City of Mexico, he stretched out naked in the bed and ask me to rub his back" [p. 3]. The municipal president filed a criminal complaint against the newspaper director for the crime of "attacks on private life," which concluded with a conviction of three years, one month and fifteen days of imprisonment for this crime. A determining element of the criminal conviction was that the press report concerned matters of a sexual nature that the authorities considered were an intangible part of the complainant's private life; the ruling was affirmed on appeal. The First Chamber of the Supreme Court reversed this ruling and declared unconstitutional the law on which the criminal conviction was founded on. More info [here](#).

xiii. Publication of personal tax data without authorization of its owner

ECtHR: In the case of *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* (2017), the Grand Chamber of the ECtHR found no violation of the right to freedom of expression after Finnish courts and authorities had prohibited two companies from processing personal tax data in the manner and to the extent that they had. The companies had collected and published information about the earned and unearned income and taxable net assets of 1.2. million natural persons in Finland, first through a newspaper and later through a text-messaging service by which people could text someone's name to a service number and receive that person's taxation information. In these circumstances, the Grand Chamber gave a wide margin of appreciation to the domestic authorities in balancing the right to freedom of expression against the right to respect for private life. The

Grand Chamber could not find that the publication of the tax data *en masse*, in this case, contributed to a debate of public interest. It also noted that although (and rather exceptionally) certain tax data was publicly accessible in Finland, a distinction was to be drawn between this accessibility and the unlimited extent to which the data was published by the companies as it rendered the data accessible in a manner, and to an extent, not intended by the legislator. The Court concluded that the restrictions were prescribed by law and pursued the legitimate aim of protecting the right to privacy of taxpayers. More info [here](#).

xiv. Classification of information regarding the impeachment of judges

Ghana: In the case of *Justice Dery v. Tiger Eye (2016)*, the Supreme Court of Ghana ruled that article 146(8) of the Constitution mandating that the processes for the impeachment of judges be held in camera prohibited publication of information related to those processes. The Chief Justice and a private company had publicized the names and details of a petition for the removal of a Judge of the Supreme Court accused of bribery and corruption. The Judge approached the Court, arguing that the publication infringed the Constitution and that this rendered the impeachment process null and void. The Court held that the disclosure of names prior to the Chief Justice's decision whether a prima facie case for impeachment was made out, violated article 146(8) but that this did not invalidate the entire impeachment process. The Court emphasized the need to balance the right to privacy and confidentiality of the judge with the right of the State to investigate allegations made against judges. It also stressed that the restriction on publication of impeachment processes was limited to the period of the impeachment, and that any permanent injunction against publication would stifle the right to freedom of expression. More info [here](#).

The application before the Grand Chamber arose from the refusal of two police departments to disclose to a Hungarian NGO the names of their appointed public defenders and the number of the public defenders' respective appointments.

xv. Public officials' personal information contained in official records

ECtHR: In the case of *Magyar Helsinki Bizottsag v. Hungary (2016)* the Grand Chamber of the ECtHR, in a majority ruling, held that while Article 10 ECHR does not confer on the individual a general right of access to information held by public authorities, such a right may arise in certain cases. The application before the Grand Chamber arose from the refusal of two police departments to disclose to a Hungarian NGO the names of their appointed public defenders and the number of the public defenders' respective appointments. The Grand Chamber determined that the access to information that was refused in this case was instrumental for the NGO's exercise of their right to freedom of expression, and met the threshold criteria that have to be met for a refusal to engage Article 10 ECHR. The Grand Chamber went on to find that the police departments' refusal to disclose the information was not necessary in a democratic society, and therefore amounted to a violation of the NGO's right to freedom of expression. More info [here](#).

In the case of *Center for Democracy and the Rule of Law v. Ukraine* (2020), the Fifth Section of the ECtHR unanimously found that a refusal by the Ukrainian authorities to give NGOs access to information about the education and work history of top politicians as contained in their official CVs, filed as candidates for Parliament, violated the NGO's right of access to public documents under Article 10 ECHR. In this judgment, the Court highlighted that it was the first case from Ukraine on access to information since the Grand Chamber's seminal 2016 *Magyar Helsinki Bizottság v. Hungary* judgment, and that it raised "novel" issues for Ukraine's authorities and courts. In its arguments, the Court applied a strict scrutiny under Article 10, recognizing the importance of transparency on matters of public interest. More info [here](#).

Paraguay: In the case of *Office of the Ombudsman v. Municipality of San Lorenzo* (2013), the Supreme Court of Paraguay granted access to the Ombudsman on behalf of a requesting party for disclosure of financial information pertaining to a number of public officials working for the municipality of San Lorenzo. The Ombudsman had argued that the refusal was contrary to Article 28 of the Constitution regarding the right to be informed as well as the country's human rights obligations under the American Convention on Human Rights (ACHR) and International Covenant on Civil and Political Rights (ICCPR). The Supreme Court referred to the Private Information Act which at Article 5 provides that data revealing natural or legal persons' financial situation may only be released: "(c) where they are contained in public sources of information." In the Court's view, "public sources of information are the three branches of the people's government; or more precisely, the documents in their possession and the persons performing public duties in these three branches." More info [here](#).

Brazil: In the case of *Gazeta de Povo v. Baptista et. al.* (2016), Judge Rosa Weber of the Supreme Court of Brazil halted several dozen privacy cases that had been brought against a newspaper and its journalists by judges who claimed that their right to privacy had been violated. The cases were brought following newspaper reports that published and criticized the judges' salaries. In a coordinated action, the judges had launched their claims in far-flung corners of the State requiring the journalists to travel thousands of miles, imposing a heavy financial burden on the defense and making it hard for the journalists to continue their day-to-day reporting. According to Judge Weber, Brazil's constitutional democratic order does not permit excessive burdens to be placed on individuals or publishers who criticize the functioning of public officials. More info [here](#).

India: In the case of *State of Uttar Pradesh v. Narain* (1975), the Supreme Court of India upheld the High Court's decision to disclose a government record. Raj Narain requested the government of the State of Uttar Pradesh to disclose the document "Blue Book" which contained security guidelines regarding the Prime Minister of India's travel. Government officials declined to produce the document, claiming that it was an unpublished official record and against the public interest. The Court reasoned that the document was not an unpublished official record since the government official failed to file an affidavit to claim it as such. In addition, the Court reasoned that it had the authority to determine whether a document is of public interest. More info [here](#).

xvi. Salaries of public officials

Venezuela: In the case of *Asociación Civil Espacio Público v. Contraloría General de la República* (2010), the Constitutional Chamber of the Supreme Court of Venezuela dismissed an action to enforce constitutional rights filed by the Espacio Público Civic Association against the refusal from the Office of the Comptroller General of the Republic to provide information about the salaries of public officials working at the institution. The Court based its decision on its analysis that the information was part of the officials' realm of "economic privacy" and that the appellants had not shown their legitimate and sufficient personal interest in attaining information belonging to this realm of privacy.

This ruling illustrates the perils of the absence of independence of the judicial power. In this case, the Supreme Court of Venezuela departs from the principle of safeguarding the right of access to information as enshrined in the Constitution and international human right standards by which access to public information shouldn't be conditioned to the applicant proving the existence of a personal or individual interest in such information More info [here](#).

xvii. Consumer Privacy

United States: In the case of *Barr. v. American Assoc. of Political Consultants* (2020), the Supreme Court of the United States held that the exception carved out to allow robocalls for collection of government debt was unconstitutional and should be severed from the remainder of the statute. Robocalls had been restricted in 1991 through the enactment of the Telephone Consumer Protection Act, but an exception was added in 2015 which allowed robocalls "made solely to collect a debt owed to or guaranteed by the United States." A group of organizations that participated in political advocacy challenged the robocall restriction, arguing that it violated their First Amendment rights by preventing them from using robocalls to communicate their political messages efficiently. The Supreme Court found the exception was an unjustifiable content-based restriction and hence could not survive strict scrutiny. It therefore severed that exception but kept the broad restriction on the use of robocalls intact, recognizing "Congress's continuing interest in protecting consumer privacy." More info [here](#).

The European Court of Human Rights (ECtHR) held that the state of Romania breached the right to privacy of the applicant when its domestic courts argued that a company was not civilly liable for broadcasting on television an interview of the applicant, then aged eleven, without the consent of her parents.

xviii. Rights of children

ECtHR: In the case of *I.V.T. v. Romania* (2022), the Fourth Section of the European Court of Human Rights (ECtHR) held that the state of Romania breached the right to privacy of the applicant when its domestic courts argued that a company was not civilly liable for broadcasting on television an interview of the applicant, then aged eleven, without the consent of her parents.

Higher domestic courts in Romania considered that the company's freedom of expression outweighed the minor's right to privacy, especially since the broadcast reported on matters of public interest. The ECtHR considered that national courts failed to correctly balance the aforementioned rights. For this Tribunal, the young age and lack of notoriety of the applicant, compounded by the little contribution that her interview was likely to bring to a debate of public interest—regarding an event she didn't witness—the absence of parental consent, and the particular interest in the protection of the private life of minors, were sufficiently strong reasons for the ECtHR to consider that Romania had breached Article 8 of the European Convention on Human Rights (ECHR). More info [here](#).

In the *Case of N.Š. v. Croatia (2020)*, the First Section of the ECtHR found that the criminal conviction of a grandmother for breaching the confidentiality of administrative custody proceedings violated her freedom of expression. The case concerned Ms. N.Š.' participation in a television interview where details about the administrative custody proceedings concerning her granddaughter were disclosed, including her granddaughter's name. She was criminally convicted for disclosing information that had been confidential, despite claims that she informed the journalists not to publicize such information and despite prior instances where the same information was publicized in the media. The Zagreb Municipal Criminal Court dismissed the applicant's proposals to hear further evidence on these claims. Her conviction was upheld by the Zagreb County Court and the Constitutional Court. The European Court of Human Rights held that, ultimately, an extensive balancing exercise was needed between the competing rights of freedom of expression and the privacy of the child. The domestic courts failed to properly conduct this exercise, instead engaging in too "formalistic" an approach. The Court found Ms. N.Š.' freedom of expression under Article 10 of the European Convention of Human Rights was violated. More info [here](#).

Colombia: In the case of *Morelli v. Noticias Uno (2013)*, the Constitutional Court of Colombia found that orders restraining the reporting of a dispute between a state official and her neighbors were over-broad for the purpose of protecting the rights of that official's child. The issue surrounded a news broadcast which included identifiable images of the official's son. The Constitutional Court of Colombia held that the rights of the child could be sufficiently protected by the removal of the images, but that it was a violation of the right to freedom of expression to order the removal of the entire news broadcast, as well as those references to the official's son that were already in the public domain. More info [here](#).

United Kingdom: In the case of *Murray v. Big Pictures Limited (2008)*, the Supreme Court of the United Kingdom unanimously allowed the appeal brought by the Appellant against the High Court's order and reinstated a claim for breach of privacy in a case wherein the photograph of a celebrity's child was taken and published without consent. The case arose when a photographer from Big Pictures Limited took the picture of Dr Neil and Joanne Murray's son, David Murray without their consent. The photograph was subsequently published in several newspapers and magazines. David's parents initiated proceedings against the photographer and Big Pictures claiming the violation of the right to privacy of their son. The High Court dismissed their appeal

and delivered judgment in favour of the Defendant. The Supreme Court allowed the appeal and observed that David had a reasonable expectation of privacy since David would not have been photographed if he had not been the son of a famous person. The Court also opined that even quotidian acts of family recreation, in public places, could be adversely affected by intrusive media attention. More info [here](#).

United States: In the case of *Globe Newspaper Co. v. Superior Court* (1982), the Supreme Court of the United States found that a Massachusetts statute that required that the public be excluded from the courtroom during the testimony of minor victims in a sex-offense trial violated the First Amendment. The case arose after Globe Newspaper Co. challenged the Massachusetts statute when it was denied access to a rape trial conducted in the Superior Court for the County of Norfolk. In its decision, the Supreme Court noted that the right of access to criminal trials was afforded protection by the First Amendment because such trials had historically been open to the press and public and because such right played a particularly significant role in the functioning of the judicial process and the government. The Court emphasized that for the constitutional right to be restricted, the State must show that denial of such a right is necessitated by a compelling governmental interest and is narrowly tailored to serve that interest. By applying strict scrutiny, the Court concluded that while the State's interest in protecting minors was compelling, it did not justify a mandatory closure rule since the particular circumstances of the case could affect the significance of the interest. Rather than a blanket closure rule, the Court deemed that the interest could be served by requiring the trial court to evaluate the need for closure on a case-by-case basis. Additionally, the Court determined that there was no evidence the rule would lead to an increase in the number of minor sex victims coming forward. More info [here](#).

xix. Privacy and public interest in the reporting of criminal cases

ECtHR: In the case of *Egeland and Hanseid v. Norway* (2009), on April 16, 2009, the Grand Chamber of the European Court of Human Rights (ECtHR) found that the Norwegian Supreme Court judgment convicting and fining two journalists for publishing photographs of a convicted criminal leaving a court building did not violate Article 10 of the European Convention of Human Rights (ECHR). The case arose after the journalists were charged under a Norwegian provision that made it an offense to photograph defendants in criminal proceedings on their way to or from a court without their consent unless there were special reasons for making an exception. While the journalists were acquitted in the first instance, the Supreme Court, which based its decision on the need to protect privacy and safeguard due process, convicted the applicants and ordered them to pay 10,000 Norwegian kroner in fines with 15 days imprisonment in default.

In its decision, the ECtHR emphasized that since Norway was not in an isolated position concerning the prohibition of photographing charged or convicted persons in connection with court proceedings, it could not be said there was a European consensus to such effect. Thus, the Court granted the competent authorities in Norway a wide margin of appreciation in balancing the conflicting interests. The Court determined that the interests in restricting the publication of the photographs outweighed those of the press in informing the public on a matter of public concern.

Further, the Court emphasized that the fact that the photographs portrayed the convict in distress and a reduced state of control meant that the need to protect her privacy outweighed the need for press freedom. More info [here](#).

United States: In the case of *Florida Star v. B. J. F. (1989)*, the Supreme Court of the United States held that imposing damages on a newspaper for publishing an article detailing the facts of a sexual assault case, including the victim's full name, violated the First Amendment. The case arose after the Appellee, B.J.F., reported a robbery and sexual assault to the Duval County, Florida, Sheriff's Department. When the department placed a copy of B.J.F.'s police report, it was obtained and later published by the Appellant, The *Florida Star*, a local newspaper. Subsequently, the Appellee filed a suit claiming that the newspaper had violated the state statute prohibiting the publication of the name of sexual assault victims. The Circuit Court of Duval County found that the *Florida Star* had violated the statute, and the jury awarded 100,000 dollars in damages to the Appellee. The Court of Appeals confirmed the decision, and the Florida Supreme Court declined to review the case; as a result, the *Florida Star* appealed to the Supreme Court. According to the Court, since the article contained accurate facts and the newspaper had lawfully obtained the victim's name from the government, imposing liability on the newspaper did not serve a "need to further a state interest of the highest order." The Court considered that although the interests in protecting the privacy and safety of sexual assault victims and in encouraging them to report offenses without fear of exposure were highly significant, imposing liability on the newspaper was too precipitous a means of advancing those interests. More info [here](#).

In the case of *Cox Broadcasting Corp. v. Cohn (1975)*, the Supreme Court of the United States held the Georgia Statute unconstitutional for making the publication of a deceased rape victim's name a misdemeanor offence. A reporter for the Cox Broadcasting Television Network broadcasted the name of a deceased rape victim while reporting the judicial trial of the incident. The father of the deceased, Cohn, brought damages action against the Cox Broadcasting Television Network claiming violation of his daughter's right to privacy under the Georgia Statute that stipulated the publication or broadcasting of the name or identity of a rape victim as a misdemeanor offence. The Supreme Court of the United States reversed the Georgia Supreme Court decision and observed that the commission of a crime and judicial proceedings arising from the prosecutions were events of legitimate concern to the public and fell within the press's responsibility to report the operations of government. It observed that the identity of the rape victim was lawfully obtained from publicly available judicial records. The Court further reasoned that restricting freedom of the press in this backdrop would be against the public interest and in violation of the Constitution. It observed that the interest in privacy faded as the published information had already appeared on the public record. More info [here](#).

Germany: In the *Case of Lebach (1973)*, the First division of the German Federal Constitutional Court held that the Court of Appeals' decision violated the fundamental rights of the complainant under Article 2(1) in conjunction with Article 1(1) of the German Constitution. The Constitutional Court reversed the Court of Appeals' decision; granting an injunction on the

broadcasting of a documentary that depicted the life and identity of a man involved in an armed robbery. The Court determined that the broadcasting of the documentary was a disproportionate interference since it included information that identified the applicant. The case arose after a German television channel commissioned a documentary about an armed robbery of an arsenal of the German armed forces where several soldiers were killed or severely wounded. The documentary referenced the petitioner's name and homosexual tendencies. When the documentary was commissioned, the petitioner had already served two-thirds of his sentence for his involvement in the robbery. The Court held that the passage of time had eroded the newsworthy character of the original crime, thus heightening the complainant's interest in his reputation and privacy. According to the Court, the human dignity and personality clauses guarantee the right "to be let alone" safeguarding the right to one's possession of his image and spoken words. More info [here](#).

 Global Freedom of Expression
COLUMBIA UNIVERSITY