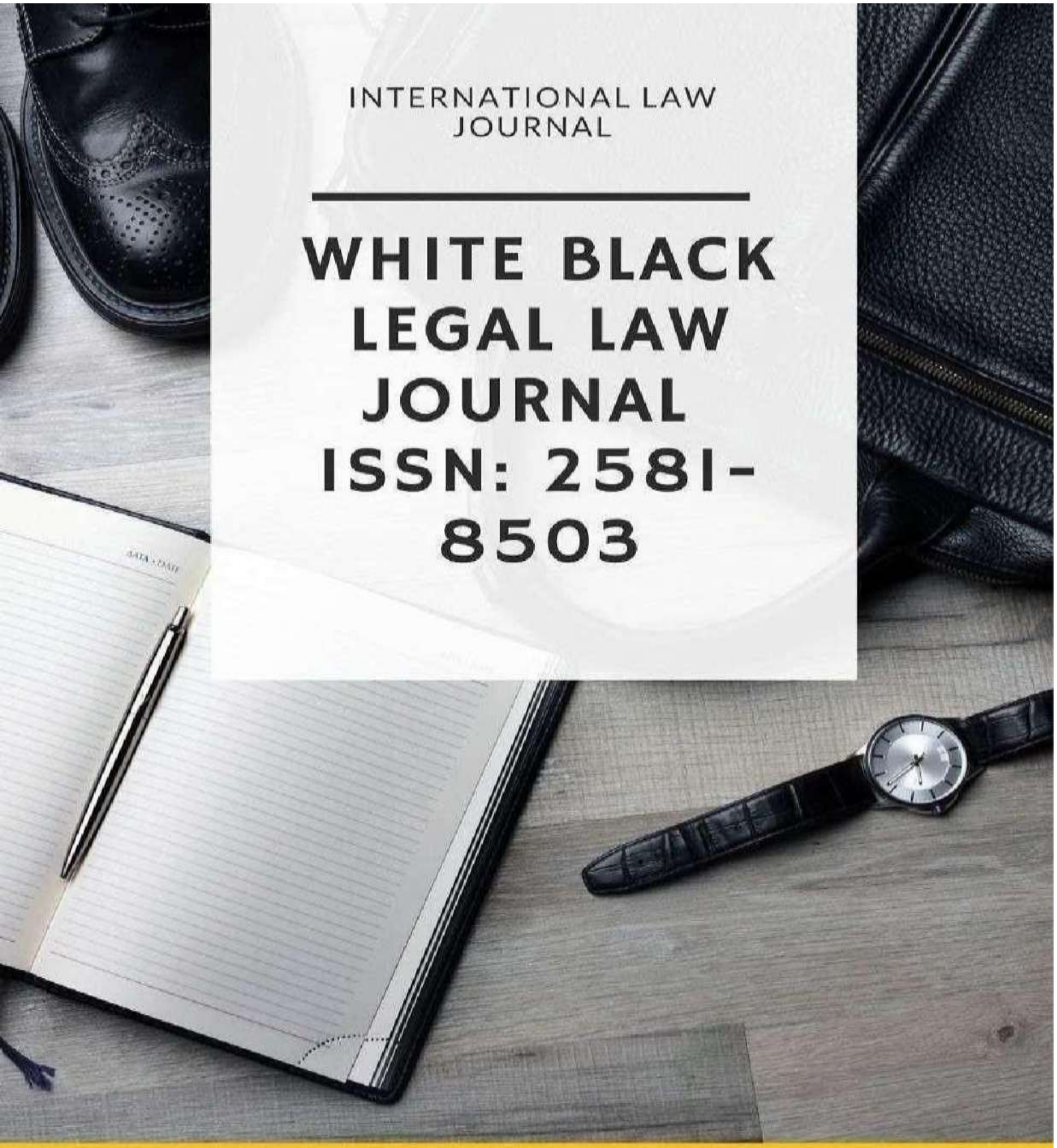

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

THE INTERSECTION OF PRIVACY AND FREE SPEECH: ANALYSING CONSTITUTIONAL PROTECTION AND LEGAL CONFLICTS IN DEMOCRATIC SOCIETIES

AUTHORED BY - KUMUD YADAV
Currently Pursuing BBA LLB (Hons.)
Amity Law School, Amity University Noida, Uttar Pradesh.

CO-AUTHOR - MS. MANVI DUTTA
Assistant Professor
Amity Law School, Amity University Noida, Uttar Pradesh.

ABSTRACT

Privacy and free speech are crucial elements for any democratic society to thrive. The exercise of both rights in conjunction, however, poses legal, constitutional, and ethical problems that challenge legislators, judges, and citizens. This dissertation will examine the legal issues created by the intersection of privacy and free speech from the perspective of constitutional law in democratic societies, including the United States, United Kingdom, European Union, and India.

The dissertation will trace the history of both rights and explore their foundations based on relevant judicial decisions and amendments to constitutions and laws in democratic countries around the world. The work will highlight key differences in balancing these rights among various democratic societies depending on whether they employ a liberty- based or a dignity-based approach.

In particular, the paper will discuss cases where privacy interests clash with free speech, for example, when governments violate individuals' private life in order to monitor and control their free expression, when media violates the right to privacy while pursuing the free flow of information, when governments collect personal data for the purpose of exercising free access to information, and other similar cases arising from the development of new technology and digitalization.

By analyzing the relevant case law, the dissertation will explore existing solutions for resolving these legal dilemmas and assess the gaps and flaws in them. Finally, the paper will evaluate the potential for developing a new strategy based on existing solutions and the current technological development.

Key findings show that there is no universally applicable solution to the problems in question. Democratic societies need to develop solutions that will be proportionate and effective within the specific context and subject to adequate supervision.

CHAPTER 1 INTRODUCTION

Privacy and free speech are crucial elements for any democratic society to thrive. The exercise of both rights in conjunction, however, poses legal, constitutional, and ethical problems that challenge legislators, judges, and citizens. This dissertation will examine the legal issues created by the intersection of privacy and free speech from the perspective of constitutional law in democratic societies, including the United States, United Kingdom, European Union, and India.

The dissertation will trace the history of both rights and explore their foundations based on relevant judicial decisions and amendments to constitutions and laws in democratic countries around the world. The work will highlight key differences in balancing these rights among various democratic societies depending on whether they employ a liberty- based or a dignity-based approach.

In particular, the paper will discuss cases where privacy interests clash with free speech, for example, when governments violate individuals' private life in order to monitor and control their free expression, when media violates the right to privacy while pursuing the free flow of information, when governments collect personal data for the purpose of exercising free access to information, and other similar cases arising from the development of new technology and digitalization.

By analyzing the relevant case law, the dissertation will explore existing solutions for resolving these legal dilemmas and assess the gaps and flaws in them. Finally, the paper will evaluate the potential for developing a new strategy based on existing solutions and the current technological development.

Key findings show that there is no universally applicable solution to the problems in question. Democratic societies need to develop solutions that will be proportionate and effective within the specific context and subject to adequate supervision. The right to privacy and freedom of expression are essential components for every democratic society to exist successfully. However, the practice of exercising those two rights leads to constitutional, legal, and ethical challenges for legislators, judges, and even citizens. This dissertation will review some of the legal challenges associated with the intersection of those two fundamental rights from the standpoint of constitutional law in democratic societies, such as the US, the UK, EU, and India.

This research will focus on the history of both rights and their grounds based on judicial decisions and changes made to respective national constitutions and legislation. Moreover, special attention will be paid to the different approaches adopted by vari ous democratic societies towards the problem discussed depending on whether they apply liberty or dignity approach.

Specifically, the cases will be considered when the right to privacy comes into conflict with free speech when governments breach individual privacy to observe and regulate freedom of expression, when media breaches individual privacy to ensure the free exchange of information, when governments obtain personal data for the sake of freedom of information, and other cases emerging due to new technologies.

Analyzing the pertinent case law, possible solutions to resolve the legal challenges will be considered, and some gaps and flaws of those solutions will be revealed. Finally, the possibility of designing a new strategy on the basis of already implemented strategies will be discussed in the context of existing technological advances.

According to the research, there is no universal solution to the problems considered. Each democratic society needs to devise a solution which will be adequate to a certain context and subject to supervision.

CHAPTER 2

LITERATURE REVIEW AND THEORETICAL FRAMEWORK

In her famous 1890 article, Warren and Brandeis argued for the right to privacy, explaining its significance to dignity, autonomy, and control over personal information. This theory recognized the changing nature of the privacy threat due to developments in technology such as photography, the emergence of popular newspapers, and the invention of the telephone. Understanding the relationship between free speech and privacy requires an appreciation of the various theories explaining both rights and their tensions. This chapter explores existing literature and theories to formulate the analytical framework guiding the entire study.

2.1 Theoretical foundations of freedom of expression

Freedom of expression rests on several theoretical justifications. These theories differ in terms of how they understand the scope of the right. For instance, the so-called marketplace theory holds that truth emerges from competing ideas and that government ought not to determine which ideas are true and which are not. Under the marketplace approach, even dangerous and incorrect ideas require protection because restricting freedom of expression poses more harm to society. This approach argues that competition is vital to societal good since bad ideas will be defeated by superior ones in the competition. Therefore, freedom of expression is absolute under the marketplace approach. However, this theory assumes that everyone is equal in the marketplace of ideas and that there is a high probability that truth will eventually prevail.

According to democratic theory, citizens can self-govern provided they have information and can express themselves regarding any matters that concern them. In this context, speech relating to politics, government functions, and public policy issues enjoys the strongest protection. However, this theory allows restrictions on free speech if such restrictions promote democracy in any way. Therefore, there are internal tensions within this theory since certain types of speech can harm democratic processes and t hus warrant restrictions.

Self-fulfillment theory posits that speech serves a critical role to an individual in the realization of personal potential. According to this theory, expression is essential to identity formation, development, and self-actualization. Self-fulfillment theory provides protection to speech even if it does not serve any social purpose as long as it expresses the speaker's interests and preferences. However, self-fulfillment also recognizes the possibility that some speech might restrict other individuals' abilities to fulfill their own aspirations.

Listener's rights theory provides a different justification for protecting expression. The core idea

is that freedom of expression implies protection for hearing others and receiving information. Under listener's rights theory, the audience has an interest in receiving information. This theory is especially useful for resisting censorship and for protecting freedom of information. This theory also recognizes the relational aspect of expression, involving communication between the audience and the speaker.

Marketplace theory supports restrictions only when speech stops people from speaking in the market of ideas. Democratic theory supports speech restrictions necessary for the protection of democratic process from subversion by disinformation or acts of violence that could undermine it. Finally, self-fulfillment allows restriction of suppression to expression that interferes with other people's self-fulfillment. These different justifications might produce different balances between free expression and other considerations.

2.2 Theoretical foundations of privacy

The theory of privacy has evolved in the course of time. Historically, liberal theories based on Locke and Mill saw privacy as a protective sphere in which an individual has the liberty to develop his or her personality without the prying eyes of the social world. This negative view of liberty is rooted in natural rights theory according to which people have the right to privacy regardless of government intervention. Twentieth-century theories, inspired by Warren and Brandeis' famous article, saw privacy as protection against new dangers associated with the use of information technology. Information became a valuable tool allowing governments to identify citizens and track them. This required protection against misuse. Information became a central part of privacy.

Privacy was increasingly seen as more than the right to be left alone. Feminists criticized the public-private dichotomy that deprived the state of jurisdiction over private matters, making it possible for domestic violence and reproductive coercion to persist unnoticed and unpunished. They pointed out that the public-private divide was inherently unjust because it made possible for power dynamics to operate beyond public scrutiny and control.

Modern surveillance theorists emphasize that information gathering and analysis lead to the creation of power dynamics and control that go beyond traditional privacy. Governments and private enterprises collecting information gain control over individuals, which manifests not only in monitoring and predicting people's actions but also manipulating them through conditioning. Individuals need not know about surveillance for its effects to take place as they become careful when they act knowing that they might be watched. Michel Foucault's notion of panopticon demonstrates this point perfectly as people behave differently when there is a

risk of being observed.

Privacy, as we have seen above, entails multiple dimensions. It covers physical body autonomy, informational control over one's data, decisional privacy, and communicational confidentiality. Freedom from surveillance is also crucial to protection. All these aspects need to be protected, and violation of one of them can lead to violations of the others.

2.3 Dignity-based vs. liberty-based frameworks

Probably the most important debate within comparative constitutional law concerns the underlying value that defines fundamental rights. Democracies are typically divided between those recognizing liberty as the key value and those recognizing dignity.

Under the liberty-based paradigm of rights interpretation, individuals' non-interference and autonomy are primary values. Under the liberty approach, any restriction of freedoms of speech must have compelling justification; the government must prove that the infringement is necessary for compelling public interests. Furthermore, restrictions on free speech and other rights must satisfy strict scrutiny. Liberty approach relies on a historical experience showing that governments frequently censor people. Trusting market mechanisms, individuals have the best ability to prevent abuse. As for privacy, the liberty paradigm considers it a negative concept – people must be free from government intrusion but have no positive right to control information. The U.S. constitutional approach to privacy is an example of the liberty model: it recognizes the right to privacy from government surveillance but not from third parties.

Dignity is the key value under the dignity paradigm of rights interpretation. Dignity is intrinsic in human beings, not granted by the government. It is the ultimate value that explains all rights, which are expressions of human dignity. According to this approach, all fundamental rights must be protected for people's mutual sake. This means that no right can infringe on the dignity of any human being. Dignity cannot be weighed against other rights or interests since they are also expressions of human dignity. Nevertheless, it can be violated if necessary for the protection of others' dignity.

The German Federal Constitutional Court is the primary proponent of the dignity approach in its jurisprudence. It holds that people's dignity is so important that freedom of speech can be restricted if it infringes on others' dignity. Similarly, it holds that privacy does not allow an individual to be free from exposure to necessary information in cases when the public interest in this information is high. At the same time, the Court recognizes the necessity of respecting other people's dignity while exercising freedom of speech. This idea stems from German historical experience when the government abused freedoms of speech.

India takes the middle position between liberty and dignity. While dignity remains the main idea of privacy and other rights, procedural aspects of the right are taken into account. For example, the Puttaswamy judgment upholds the necessity to restrict fundamental rights if it is done to achieve governmental aims and for proportionate reasons.

CHAPTER 3

CONSTITUTIONAL PROTECTIONS IN DEMOCRATIC SOCIETIES

As seen earlier, the approach to ensuring privacy and free speech differs among democratic countries based on historical experiences and national constitutional arrangements. This chapter will explore the constitutional background of protecting these two fundamental rights within major democracies, noting similarities and differences.

3.1 United States Constitutional Framework

The US Constitution offers explicit textual guarantee of free speech in its First Amendment, according to which Congress 'shall make no law... abridging the freedom of speech, or of the press'. In contrast to many other democracies, this right cannot be subject to qualification. The American constitutional law interprets the First Amendment as offering some of the broadest protection for expression possible in the democratic world. Freedom of speech in the US includes political, commercial, symbolic, and even expressive conduct. Speech may only be restricted in response to a 'compelling governmental interest' using the least restrictive measures (narrow tailoring).

The history of interpreting the First Amendment shows that the USA's legal system has a very high bar for restricting free expression. Traditionally, the Court held that speech could only be regulated if it constituted 'imminent lawless action'. This posit ion evolved until Brandenburg v. Ohio case set the current precedent: speech can be restricted only if it was directed at 'inciting or producing imminent lawless action' and it would probably lead to such action. Such a restrictive approach reflects the American idea that the danger from suppressing expression outweighs the danger posed by unrestricted speech. The famous New York Times v. Sullivan established the standard for punishing officials who had suffered reputational damage due to an article written about their actions: public officials may claim defamation only if they proved actual malice in writing the article (knowing falsity or reckless disregard for the truth). Other controversial rulings showed that Americans prioritize freedom of speech even if the expression of views was offensive, false, or damaging emotionally.

Unlike freedom of speech, the right to privacy has no constitutional foundation. The US Supreme Court found it in different constitutional provisions, most notably the Fourteenth Amendment's due process clause. According to the American judiciary, the right to privacy includes the right to personal physical autonomy and the right to make certain kinds of decisions. The right was first recognized in Roe v. Wade ruling that guaranteed reproductive autonomy. Later, Lawrence v. Texas established the right to decide matters of intimate character. However, the Court did not recognize informational privacy as a constitutional right. Instead, American legislatures passed various sectoral laws regulating the collection and dissemination of sensitive information (health information, financial information, or information about children online). Restrictions on government surveillance were exceptionally difficult to meet because they imposed a heavy burden of proof on the plaintiff.

3.2 United Kingdom and European Framework

While the UK does not have a written constitution, it incorporated the European Convention on Human Rights into domestic law in 1998 under the Human Rights Act. Article 10 of the ECHR guarantees the right to freedom of expression including the right to hold opinions and receive, impart, or communicate information and ideas. However, under Article 10(2), restrictions can be made if it is required for the interests of the democratic society to protect the rights or reputations of others, national security, public safety, or other legitimate grounds. Similarly, Article 8 recognizes the right to respect for private and family life, home, and correspondence and also allows for restrictions in cases described in Article 10(2). In contrast to the American approach, the ECHR recognizes these rights as possibly conflicting and subject to proportionality tests.

GDPR establishes data protection as a fundamental right within EU law. It confers several data subject rights, including the rights of access, rectification, erasure, data portability, etc. Companies processing data are expected to do so legally, in good faith, with appropriate transparency. For example, personal data cannot be transferred outside the European Economic Area without consent of the individual involved or authorization from EU authorities. Under GDPR, organizations can be fined heavily, as much as up to €20 million or 4% of the global annual revenue, whichever is higher. While the GDPR contains exceptions for processing that serves the exercise of freedom of expression and information, they require balancing with other rights, which makes GDPR different from the American approach of virtually unlimited free expression.

Under the new Digital Services Act, digital service providers now have new obligations that

ensure respect for the right to free expression online. For example, Very Large Online Platforms need to identify content that poses risks to users, including fundamental rights. They should develop a risk management strategy and conduct annual independent audits, with possible sanctions being a fine of up to 6% of global annual revenue and operational changes for the platform in question. Meanwhile, under the UK Online Safety Act (passed in 2023), digital services have to carry out statutory duties, including assessing, mitigating, and managing content risks. This includes illegal content (terrorist material, child abuse images), prohibited content (hate speech, extreme pornography), or harmful content categories (e.g., bullying content). Non-compliance can result in severe penalties, such as imposing Ofcom fines worth up to £18 million or 10% of global annual turnover.

3.3 Indian Constitutional Framework

Freedom of speech and expression is explicitly mentioned in Article 19(1)(a) of the Constitution of India. However, unlike the US constitutional law, this fundamental right is subject to reasonable restrictions described in Article 19(2). These restrictions include actions necessary for securing the sovereignty and integrity of India, national security, friendly relations with foreign states, and others. In sum, India takes a middle approach to freedom of speech by allowing for some restrictions in particular cases.

In practice, the Indian Supreme Court made a number of progressive rulings that interpret freedom of speech. In 1989 S. Rangarajan v. P. Jagjivan Ram case, for instance, the Court held that speech could be censored if and only if the 'remedy of more speech' was unavailable. In the 2015 Shreya Singhal v. Union of India case, the Indian judiciary invalidated Section 66A of the Information Technology Act 2000 as unconstitutional because of vagueness and overbreadth. Notably, this ruling extended free speech protections to include online communication and emphasized the importance of narrowly defining restrictions and avoiding arbitrary enforcement.

Although the right to privacy has no explicit constitutional protection in the 1950 Indian Constitution, it was gradually established as an integral part of the right to life and personal liberty (Article 21). As the case in point, the Supreme Court held in 2017 in Justice K.S. Puttaswamy v. Union of India that privacy was indeed a fundamental right. In accordance with this ruling, to regulate privacy, the legislation must pass a three-fold test that includes proving legality, necessity, and proportionality of the measure (i.e., a rational connection between the goal pursued and the measure adopted). This test applies equally to free speech, thus providing a way to balance competing interests. More recently, in 2023, in Kaushal Kishor v. The State

Of Uttarakhand, the Indian Court ruled that fundamental rights of Articles 19 and 21 were applicable in a horizontal sense against private parties as well.

CHAPTER 4

PRIVACY RIGHTS: EVOLUTION AND CONTEMPORARY SCOPE

It is somewhat surprising to note that the legal concept of privacy is a relatively modern one. Until the late nineteenth century, there was no term for 'right to privacy' within legal discourse. Even after then, it was only much later that explicit consti tutional protection emerged for privacy rights. Nevertheless, privacy concerns have existed for as long as human beings needed autonomy, personal freedom, and space free of surveillance. This chapter will examine the historical evolution of privacy from philosophy into constitutional law and will analyze different contemporary dimensions of privacy.

4.1 Historical Evolution and Philosophical Roots

Philosophical roots of privacy can be found in early notions of shame, honor, or personal dignity. Nevertheless, the development of the modern notion of privacy was triggered by new technologies. New inventions such as photography and telegraph in the nineteenth century created new opportunities for violation of privacy through intrusions into personal intimate spaces. Legal scholars were thus prompted to create a theory of privacy. In their now-famous article, The Right to Privacy, Samuel Warren and Louis Brandeis argue that the notion of an implicit privacy right exists within common law because of the need to protect individuals from new technologies and dissemination of information about private individuals. In particular, they wrote that 'the intensity and complexity of life, attendant upon advancing civilization, has rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual'. This quotation is still relevant today and implies that advances in technology make the protection of privacy increasingly important.

The twentieth century saw the gradual expansion of the notion of privacy from tort law into constitutional law and the provision of protections of various kinds against government and third parties violating the privacy rights. American courts provided legal protection against intrusion upon seclusion, appropriation of an individual's name or likeness, public disclosure of private facts, and false light in the public eye. These torts provided protection of an individual's privacy against third parties. Constitutional protections for privacy included a right to abortion

established in Roe v. Wade (1973). In this case, the Supreme Court identified constitutional privacy right, protected by the Due Process Clause. The right related to issues concerning reproduction and was grounded in personal autonomy. In this way, the case also hinted at a wider privacy right beyond the field of procreation.

In Lawrence v. Texas (2003), the Supreme Court further extended the constitutional privacy rights to cover intimate choices about one's sexuality. Namely, in that case, the Court argued that the State cannot interfere in private decisions that affect intimate relationships. The Court has not recognized, however, a broader privacy right that covers informational privacy, i.e., who controls personal data. The Supreme Court has been rather accommodating to the government's need to collect personal data for surveillance, national security, and law enforcement.

4.2 Contemporary Dimensions of Privacy

Several dimensions of privacy exist in contemporary society. Each dimension of privacy concerns distinct interests. Bodily privacy prevents individuals from any physical invasion of their body or any unwanted touching. This type of privacy is connected with protecting reproductive and health-related choices, medical care, and freedom from non-consensual searches. Territorial privacy is concerned with preventing any intrusions or surveillance of homes and intimate spaces. It is based on the idea that individuals need a territory that would protect them from observation and allow them to engage in intimate activities without the threat of surveillance. Homes are especially important within privacy laws of all democracies and receive heightened protection.

Decisional privacy provides protection to individuals making intimate decisions about their lives, such as having children, making decisions about sexuality, getting married, and building family lives. These decisions are considered to be so personal that they do not belong to the realm of government's concerns even if regulating them would be justifiable on other grounds.

Informational privacy is the most important dimension in the modern society due to the importance of collecting personal data. It concerns personal information such as individual names, addresses, location data, medical and genetic information, personal financial information, and so forth. Such information is usually collected by governments, businesses, and institutions, and individuals have very limited control over its collection. Aggregating large amounts of personal information can allow discovering sensitive information such as political views, sexual orientation, financial situation, etc. The General Data Protection Regulation (GDPR) and similar legislation address this privacy dimension.

Communicational privacy is concerned with preventing any interception or unauthorized release of any communication, including letters, phone calls, emails, and other means. This is an especially crucial dimension because communicating privately with others is essential for developing personal relationships free of state intervention. Relational privacy deals with the issue of protecting relationships from unwanted intrusions. Relationships such as marriages and intimate relations depend on some level of privacy to thrive. Disclosing personal communications with others and intimate relations themselves can hurt the quality of such relationships.

New dimensions of privacy have emerged recently. Algorithmic privacy is concerned with prevention of any decisions made by companies or governments using algorithms and relying on personal information. Using an algorithm to determine whether the person is trustworthy, suitable for a job, for parole or release, or even what content to display to an internet user poses significant dangers of discrimination and manipulation. People may not know how the decisions are reached. Associational privacy is the protection from revealing information about one's connections and associations. Revealing information about individuals associating with one another can provide the government or businesses with valuable data on individuals' politics, religion, and other information.

Digital technologies also present new threats to relational privacy and territorial privacy. For instance, geotagging allows identifying the location of people and discovering any patterns of their movement. Digital networking provides an opportunity to map people's connections and interactions.

4.3 Privacy as Prerequisite for Expression and Democracy

Modern scholarship revealed that privacy and freedom of expression are interdependent rather than mutually exclusive. Indeed, the latter cannot be achieved without privacy. An individual needs an opportunity to explore one's own personal opinions without any government intervention. Without this kind of opportunity, it is impossible to develop one's political, ethical, or religious views. Any surveillance creates fear in the individual and discourages expressing any views out of fear of retaliation or punishment.

Surveillance can create a chilling effect on expression. Studies show that when individuals are aware that they are under surveillance, their behavior changes and they tend to avoid engaging in any controversial activities. Thus, it becomes almost impossible to express any opinions that might be considered controversial.

This dynamic is especially relevant to journalists, human rights defenders, and activists of

various kinds. Journalists cannot operate if any contacts are under surveillance. Similarly, human rights defenders will find it difficult to investigate cases if all their communications are surveilled. The same applies to activists. The ability to communicate freely is a necessary condition for their work. Investigative journalism, documenting human rights violations, and organizing activities are all impossible without the assurance that communications are secure.

Furthermore, a democracy cannot function without either right. For instance, people cannot freely participate in democratic processes if the State constantly monitors all their actions and communications. On the other hand, democracy requires access to inf ormation and freedom of discussion. Freedom of expression is an important component of any democratic process. As UN Special Rapporteur on freedom of opinion and expression has stated, communications surveillance is a highly intrusive activity that interferes with both privacy and freedom of expression. Therefore, democratic laws need to recognize the tension between the two rights.

CHAPTER 5
FREEDOM OF EXPRESSION: DEFINITIONS AND BOUNDARIES

While the freedom of expression covers much more than the freedom to express one's opinion, it also includes the right to have such an opinion, obtain information, and participate in public debate. Still, every democracy defines limits to the right to freedom of expression. The exact limits vary significantly between democratic states. In this chapter, we discuss how democratic states define expression and determine the extent of its protection as well as the restrictions that can be legally applied.

5.1 Scope of Protected Expression

Protection granted by democracies to various forms of communications differs. Political speech, i.e., communication about politics, elections, and public policies is the highest protected form of expression in most democracies due to the core idea of democracy – citizens' self-government. Criticism of governmental leaders, discussion of policies, and participation in election process represent the key examples of politically valuable forms of expression. Religious speech, associated with the question of spiritual truth and personal ethical beliefs, receives increased protection as well as art and cultural expression since both are vital for the societal self-understanding and personal/cultural development. Protection of artistic and obscene expression is controversial among democracies.

Scientific/academic discourse is another type of expression that requires protection from

governmental interference since it facilitates searching for knowledge and truth. Universities and scientific organizations recognize the importance of academic freedom in their activities. Advertising or any other form of commercial speech requires protection of commercial expression as well since many democracies allow regulating it. At least the restriction of commercial speech in cases of misrepresentation and deception can be considered valid. Symbolic speech that involves the use of expressive conduct rather than words also receives protection of freedom of expression. Flag-burning, wearing armbands as a sign of protest are examples of symbolic speech.

It is not difficult to determine the limits of speech in general; however, it may be tricky to define the limits of expression. For instance, can the spending of money on campaigns serve as a form of speech that must be protected? How can nude dancing be interpreted as protected expression? Can hate speech and incitement be legally covered by this term? The answer to each question is different because there are different approaches to defining speech that deserves protection and determining the limits of its freedom.

5.2 Recognized Categories of Unprotected or Restricted Speech

Democracies recognize a few categories of speech that should either be banned entirely or regulated. Speech involving incitement to violence – speech that aims to provoke and actually does provokes an illegal act – is regulated across democracies; however, the legal threshold of incitement differs. In the US, very high standards must be met; in European jurisdictions, lower standards of proving incitement are acceptable since the latter understands that certain speech represents a real danger even though it is not immediately actionable.

Speech that represents hate and is directed against protected groups, defined according to criteria of race, ethnicity, sexual orientation, religion, and disabilities, is restricted almost everywhere except for the United States that considers all hate speech non-prohibited as long as it does not involve imminent violent consequences. In fact, European democracies experienced the totalitarianism and genocide; therefore, they were more inclined to restrict hate speech because hate speech deprives the target groups of the freedom of speech since it intimidates them with potential violence or discrimination.

Defamatory speech and speech representing lies or misstatements of facts also can be restricted to protect reputational interests of individuals since democracies grant a high value to reputation. Public figures need to prove 'actual malice' in the US while the burden of proof in other democracies is less heavy. Defamatory speech is regulated due to the same reason – protecting reputational interests of the speaker and other individuals. Pornographic speech and

obscenity are restricted because of their sexual content. Speech restrictions in relation to national security represent an exception to the rule as well. Speech representing contempt of court also can be limited since it undermines justice. Spam and deceptive commercial speech can be limited as well to protect consumers.

CHAPTER 6

THE CONFLICT BETWEEN PRIVACY AND FREE SPEECH

However, there are instances where exercising privacy and free expression leads to a conflict. This chapter identifies the core conflicts and looks into how such a conflict manifests itself in practice where democracies have to choose between either of the two rights.

6.1 Government Surveillance vs. Freedom of Expression

Governments use surveillance to monitor communication, collect information about the movement and associations of their citizens, and use surveillance technologies. This violates the privacy rights of the citizens, as mentioned earlier. Further, the mere presence of surveillance causes people to self-censor their opinions, avoid any controversy, and refrain from criticizing the government out of fear of being observed. This is particularly harmful to journalists, human rights defenders, and political activists, who require secrecy in their dealings to carry out their jobs efficiently. UN Special Rapporteur on freedom of opinion and expression recognizes that communications surveillance is an extremely intrusive process that interferes with free expression and privacy, posing a threa t to the very essence of democracy.

Democratic governments argue that surveillance is needed for national security, combating terrorism, and enforcing law. There is legitimacy in some surveillance activities but mass surveillance programs are not justified. Whistleblowers have revealed the existence of mass surveillance programs by democracies, in which the purpose of surveillance often transcends the justification. For example, the revelation of the NSA's surveillance of the German Chancellor Angela Merkel, mass collection of metadata of millions of Americans without any connection to terrorism, and European states' surveillance of their own citizens.

Here, we cannot solve the problem by sacrificing one of the rights in favor of another. Instead, democracies need to ensure appropriate legislation that allows governments to take necessary security measures but does not allow surveillance authorities to go beyond what is required, which can lead to suppression of expression of opinions and ideas. This entails that the surveillance program must have proper legal authority, legitimate aim, necessity and

proportionality requirements, judicial oversight, and transparency regarding surveillance activities. While some democracies have performed well in this area, many democracies fail to do so.

6.2 Media Freedom vs. Personal Privacy

This conflict between media freedom and privacy of individuals has always been around, with publishers arguing that they have the right to cover matters that are in the public interest and individuals maintaining that they have the right to control informa tion regarding their personal life. In the pre-digital age, this conflict took place whenever issues of privacy were connected with publishing information about a public individual, scandal associated with a public individual, or when an investigative piece revealed some wrongdoings.

An important factor in this case is whether the individual is a public or a private individual, which is an integral part of resolving this conflict. The fact that an individual is public reduces the expectation of privacy that an individual enjoys, because actions of such individuals affect the general population and the public has legitimate interests in knowing about the conduct of public individuals. Here, the issue is the extent to which privacy expectation is lowered in case of a public individual. Does it mean that all rights to privacy disappear when an individual is classified as public? This depends on each democratic state.

The German Federal Constitutional Court rules that although public figures have lessened their expectation to privacy, they have a right to privacy in relation to their family life and personal relationships. American courts have generally deferred to media by permitting publication of truthful information about public figures without proof of actual malice. Private individuals have strong claims of privacy. Here, courts have to weigh several factors to decide whether there is any violation of privacy: the relevance of the information to public matters, whether the individual is public or not, the activity in which the individual is involved, and how the information came to be known to the media. Today, this distinction becomes complicated in view of the fact that anyone has become a publisher with social media. Any individual posting something on the internet can be read and re- posted millions of times, causing the individual's personal information to become partially public in nature. At the same time, the reposting of such personal information by news agencies raises issues of newsworthiness and privacy.

6.3 Data Protection vs. Freedom of Information

With the introduction of the GDPR type of data protection laws, a whole new dimension of conflict with free expression and right to information has emerged. GDPR includes the 'right to

erasure' or 'right to be forgotten' in which the individual can ask to delete any personal information published online regarding him or her. The purpose of the right to be forgotten is that it protects the individual from having permanent digital records of facts that may no longer be relevant or truthful. The right to be forgotten comes into conflict with freedom of information when, for example, Google or any other search engine removes links of accurate information about someone contained in the newspaper articles.

The European Court of Justice, in the case of Google Spain SL v. Agencia Española de Protección de Datos, 2014, balanced these two rights by ruling that search engines should delete links of personal information from search results in cases when the inform ation is not relevant to the matter anymore. Here, it is crucial that this right to be forgotten is not an unlimited one but rather one that needs to be balanced against the right to freedom of expression, especially in situations when the personal information is relevant to matters of public interest or if the individual is a public individual.

Another area where privacy law and freedom of information law come in conflict with each other is the right of citizens to make freedom of information requests. Citizens use this right to gain access to governmental documents to keep the government transparent and responsible. The problem is that such governmental documents contain personal information about individuals. On top of that, data protection regulations prohibit governments from making personal information available or using such information in the process of processing such information requests. In some cases, governments misuse data protection laws in order to protect their misconduct from the public eye.

CHAPTER 7
CASE LAW ANALYSIS AND COMPARATIVE JURISPRUDENCE

Courts play a vital role in determining what constitutes a fundamental right and enforcing it. As can be seen from the case studies below, different jurisdictions use different approaches to resolving privacy versus free expression disputes.

7.1 American Jurisprudence: Supremacy of Free Speech

American courts are known for placing greater value on free speech than on any other fundamental right, including privacy. In New York Times Co. v. Sullivan (1964), the US Supreme Court ruled that public figures cannot obtain damage recovery for statements made regarding their official actions if it is shown that the statements were published "with knowledge

of their falsity or with reckless disregard of whether they were true or false." This stringent test reflects America's understanding that free speech supports democracy by allowing criticism of public figures, and that a few lies are better than preventing people from speaking the truth. Consequently, public figures have lower protection of reputation and privacy than in other countries.

Another example is the case Brandenburg v. Ohio (1969). The Court ruled that speech that advocates illegal actions could only lead to punishment if the advocacy was aimed at producing imminent illegal activity and there were strong indications that such activity would occur. This very strict standard of permissible speech is based on the conviction that truth will emerge in unrestricted competition in the marketplace of ideas. While similar standards have been adopted in other democracies, Brandenburg's test remains unique in its stringency.

On the other hand, courts tend to apply much narrower tests in regard to protecting privacy. Thus, in Roe v. Wade (1973), the US Supreme Court found that the concept of privacy is implicit in the Constitution's Due Process clause and protects reproductive autonomy. However, the Court did not recognize privacy as a general fundamental right, let alone one covering informational aspects of privacy or personal data protection. In Cox Broadcasting Corp. v. Cohn (1975), the Court ruled that states cannot prohibit the press from publishing information that is obtained lawfully, even if the information invasion of a person's privacy. It refused to impose limitations even on broadcasting the name of a woman raped because this information was in the public domain.

As can be seen, the hierarchy of constitutional rights in the USA is as follows: free speech enjoys the highest degree of protection, and privacy is relatively weak. The resolution of conflicts involves the supremacy of free speech most of the time, which can be explained by America's historical fear of government censorship and the belief in market forces to limit abuses.

7.2 European and UK Jurisprudence: Proportionality and Balance

European courts resolve conflicts between privacy and free speech using proportionality analysis as a standard procedure. According to numerous rulings of the European Court of Human Rights (ECHR), both Article 8 (right to privacy) and Article 10 (free expression) are essential for a democratic society. Therefore, the former cannot prevail over the latter in all cases. Instead, ECHR applies the doctrine of proportionality, determining whether restrictions on the exercise of either right are justified by compelling purposes and are proportionate.

One of the landmark decisions that reflect this principle was Von Hannover v. Germany (2004). The court ruled that German courts reasonably balanced the conflicting rights when they

prevented a newspaper from publishing pictures of Princess Caroline of Monaco in her private life. The reason for this decision was that she had reasonable expectation of privacy despite being photographed in a public place because her interest in privacy was stronger than the interest of the magazine in publishing photographs that were merely commercial but not of importance to the public.

Following this ruling, in subsequent cases Von Hannover v. Germany (2012), the European Court of Human Rights reiterated the principle of dignity and held that photographs published of the princess in public places where her family members were present could form grounds for compensating for damages. The reason was that she had taken sufficient measures to preserve the family's privacy from media attention.

Another interesting line of decisions of the ECHR concerns the right to be forgotten. For instance, in Google Spain SL v. Agencia Española de Protección de Datos (2014), the European Court of Human Rights ruled that the Internet user has a right to remove links leading to outdated or irrelevant information containing personal information. At the same time, this right should not interfere with free speech. Therefore, in subsequent rulings, the court has clarified which restrictions on the right to be forgott en are justified when the information relates to matters of public interest or a public figure.

As can be seen, the European approach to balancing privacy and free expression allows for treating the two as potentially equal rights and applying proportionality tests in particular cases. This strategy differs fundamentally from the American presumption of the supremacy of free speech.

7.3 Indian Jurisprudence: Emerging Framework

In India, courts have gradually built an independent approach to resolving privacy vs free speech problems in line with the country's constitution. The Constitution guarantees freedom of speech (Article 19(1)(a)) but does not mention the concept of privacy anywhere in the text. Nevertheless, courts interpret Article 21 (right to life) as implicitly guaranteeing the right to privacy.

In R. Rajagopal v. State of Tamil Nadu (1994), the Court found that unauthorized disclosure of a person's life story, if the facts are true, violates his/her right to privacy. At the same time, it recognized that public figures have lesser expectations of privacy in regard to their activities related to public affairs. The Court acknowledged that journalists may have a legitimate interest in discussing topics that are of interest to the public. Therefore, it decided that this article does not eliminate press freedom but limits its range to purely personal issues. As criteria for

balancing interests, the Court suggested considering the following issues:

Reduced privacy protection for public persons and matters of public concern.

Lower privacy protection for matters of public concern in case of invasion of privacy. Relevance of the way in which information was obtained to the protection provided.

Later decisions have refined this concept further, for instance, Puttaswamy & Others v. Union of India (2017), where the Court established that privacy is one of the basic elements of the right to life and liberty. Moreover, it set forth a three-pronged test to apply when restricting any fundamental right in order to fulfill another purpose. The test requires:

(1) That the action is authorized by law;

(2) That the action pursues a legitimate state objective;

(3) That the restriction is necessary and proportionate to achieve that objective

This bidirectional approach promises greater nuance compared to the American model of presumptive superiority of one fundamental right over another. As noted by Justice D.Y. Chandrachud in the majority opinion, a majority verdict cannot infringe on any of the fundamental rights guaranteed by the Constitution. Justice Kaul in his dissenting opinion insisted that courts need to take a non-majoritarian viewpoint for the sake of protecting minorities' rights.

In Shreya Singhal v. Union of India (2015), the Court ruled on the issue of regulating online speech and expression, overturning provisions of the Information Technology Act prohibiting sending of "grossly offensive" or "menacing" messages via electronic communications. The reason was that the terms were too vague to give the recipients sufficient notice of the prohibited action. As with other forms of expression, Internet communication enjoys full constitutional protection.

Recently, in Kaushal Kishor and Others v. Central Bureau of Investigation and Others (2023), the Court ruled that fundamental rights of citizens, including free speech and privacy, could be enforced horizontally—that is, against private persons and organizations.

CHAPTER 8

DIGITAL AGE CHALLENGES AND INTERNET GOVERNANCE

The digital revolution has brought about fundamental changes to both privacy rights and free expression rights which result in new conflicts and challenges that current legal systems cannot effectively handle. The chapter investigates important difficulties which the digital world presents while showing how different democratic systems develop their regulatory frameworks

to address these issues.

8 1 Mass Data Collection and Surveillance Digital technologies now enable organizations to collect and store personal data at an unprecedented level which they can analyze without limits. Tech companies collect user data through tracking their locations and search queries and communications and purchases and behavioral patterns without users understanding how their data will be used. Governments use surveillance technologies like facial recognition and phone tracking and internet monitoring systems which they operate with little judicial control and no public oversight. The Edward Snowden revelations demonstrated the scale of state surveillance, showing that NSA and other intelligence agencies collect telephone metadata from millions of American citizens, intercept communications internationally through cables and networks, and engage in mass surveillance programs that sweep up data of innocent people with no connection to terrorism or criminality.

These practices create new privacy dangers which go beyond established privacy protection measures. Surveillance goes beyond determining whether someone reveals a specific piece of information because it involves collecting information and creating deductions based on the collected data. The process of linking different data points enables people to discover private information about others which includes information about their beliefs and their friendships and their medical conditions and their financial situation. A person's search history reveals medical concerns and personal interests. People use location data to track their movements between home and work and church and social locations. The way people communicate with each other shows their social connections and the people they know. The process of aggregating information creates damage which exists as a separate entity from the possibility of information being disclosed.

The practice of mass surveillance creates an environment which inhibits people from expressing themselves freely. People become aware that someone is tracking their online activities which creates on them a demand to stop using the internet.

CHAPTER 9

BALANCING MECHANISMS AND LEGAL SOLUTIONS

However, addressing the tension between privacy and expression is not as simple as acknowledging that both are important. Democratic systems must create processes for balancing the conflicting claims. This chapter explores such balancing approaches and their strengths and weaknesses.

9.1 Constitutional Proportionality Tests

Proportionality testing has emerged as the leading mechanism for balancing fundamental rights among democracies. Originating in European constitutional law, proportionality analysis is now used by courts in India since Puttaswamy. The basic structure of the proportionality test involves four elements:

The first element, legitimacy, requires that the measure serves a legitimate purpose. Such purposes include protecting individual privacy, promoting national security, and safeguarding disadvantaged groups. Other measures aimed at preserving reputations or preventing offense, while recognized as legitimate aims in some democracies, will be scrutinized. Aims motivated by purely political considerations or those that seek only to preserve governmental power will fail this requirement.

The second element requires necessity, meaning that there are no less intrusive means for achieving the aim. This element discourages overbroad measures that affect many other interests unnecessarily. Any measure that could be achieved through less intrusi ve means does not satisfy this criterion. The necessity requirement calls for careful analysis of available alternatives, not perfunctory dismissal.

The third element is suitably called suitability. It requires that the means are reasonably connected with the aim pursued. In other words, the measure must actually advance the aim. Even where an aim is legitimate, a measure lacking connection to it will fail the suitability test.

Finally, narrow proportionality requires a balance between the advantages and disadvantages created by the measure. Where the interests promoted by the measure significantly outweigh the interests harmed, narrow proportionality is satisfied. Narrow proportionality is the most controversial element of the test because it calls upon courts to weigh various interests in a complex manner.

Proportionality analysis has several advantages compared to strict rules and absolute standards. It permits flexible and context-dependent balancing; focuses judges' attention on relevant

considerations; and allows for case-by-case balancing of interests. On the other hand, proportionality is extremely time-consuming, and its guidelines are limited in applicability to novel cases. Moreover, courts may apply proportionality inconsistently. Disagreements may arise regarding the weight accorded to certain criteria; the comparison of incomparable values; and whether some interests are ever weightier than others. Finally, this balancing framework poses the danger of judicial overreaching because judges engage in value judgment in applying the test.

CHAPTER 10

CONCLUSION AND FUTURE DIRECTIONS

The conflict between the right to privacy and the right to freedom of expression stands out as one of the major dilemmas facing modern democratic societies. This dissertation attempted to map the theory, constitutional law, history, and current controversies surrounding these fundamental rights. In doing so, it revealed certain general principles common to all democracies, as well as differences rooted in different constitutional systems and traditions.

10.1 Main Findings

First, contrary to the popular perception, privacy and expression rights are complementary to one another. Privacy is a necessary precondition for self-expression, for an individual must feel safe from prying eyes before she can form and articulate her views freely. At the same time, it is expression that challenges any privacy invasion practices. Democratic law must protect both rights simultaneously rather than opting for one over the other.

Second, although all democracies recognize privacy and expression, they adopt fundamentally different frameworks for balancing them. America emphasizes freedom, whereas Europeans and most Commonwealth democracies follow the principle of proportionality and treat privacy and expression as co-equal rights. India has established a unique system combining the principles of constitutional text and more advanced balancing procedures. None of these approaches is preferable over others; they represent reasonable constitutional choices made by democracies.

Third, in the digital age, these conflicts are exacerbated manifold. Technology has dramatically increased both the possibilities for expressing oneself and invading others' privacy. Traditional frameworks designed in the pre-digital era are ill-suited to address the modern challenges.

Fourth, existing constitutional and statutory law and regulatory regimes leave much to be

desired in many respects. Governmental surveillance takes place almost entirely without legal restrictions or independent oversight. Regulations for personal data protection remain fragmented and ineffective. Platforms exercise unchecked control over online expression. Algorithms make critical decisions without oversight or explanation.

Fifth, to move forward with protecting these fundamental rights, multi-leveled strategies need to be employed. Universal standards should be articulated under international human rights regimes. National legislation must guarantee protection for both rights. Courts should enforce these guarantees. Regulatory agencies must oversee surveillance activities and data management. Standardization through industry associations should be encouraged. Civil society organizations may help enforce laws and regulations.

1.2 Recommendations for Democratic Societies

From the foregoing analysis, several concrete recommendations may be offered for the benefit of democratic societies:

1. Develop integrated legal frameworks protecting both privacy and expression rights. Democracies should implement laws protecting privacy—especially informational privacy—and data. At the same time, robust protections should remain in place for free expression. The legal protection of these rights should acknowledge their interdependence.
2. Impose restrictions on government surveillance through legislation. Surveillance should take place only in compliance with strict legal standards. Surveillance for illegitimate or improper purposes violates the rule of law and creates unjustifiable restrictions on free expression. No surveillance program should escape legal authorization, oversight, and review.
3. Strengthen judicial supervision and oversight of government actions. Courts should carefully review any limitations on privacy or free expression. Proportionality analysis should be used when reviewing restrictions on these rights. Oversight boards should be established to oversee surveillance programs and personal data use. Inspections should be conducted to verify compliance with legal standards.
4. Implement regulations over platform governance. Platforms should be required to provide information on their content moderation practices and allow users to appeal decisions. Transparency in algorithmic decision-making is imperative. Competition policy should be used to break platforms' market dominance and reduce their role as expression gatekeepers.

5. Educate citizens about their digital rights and responsibilities. People must learn how their personal information is collected and processed and how to use the Internet safely.
6. Promote international cooperation in digital governance. Protection of digital privacy and expression transcends national borders, requiring cooperation on setting standards.

10.3 Conclusion

In conclusion, privacy and expression are not merely interesting philosophical concepts but concrete protections of human dignity. Individuals cannot live as autonomous people and exercise their freedoms without both rights. Ensuring that privacy and expression are adequately protected is both a legal and moral responsibility that democracies owe to their citizens.

These conflicts cannot be resolved forevermore. Rather, democracies must constantly negotiate the balance of privacy and expression as technology changes, new security or social threats arise, and societies become increasingly heterogeneous.

Such protections require not only constitutional doctrine and statutory law but also institutional innovation and democratic deliberation and commitment to protecting both rights. At stake are considerable matters. Societies that protect expression but violate privacy become societies in which surveillance silences dissent and authoritarian control is possible despite democratic institutions. Societies that protect privacy but violate expression become societies in which government censorship or monopoly control prevents democratic participation and accountability. Only societies that protect both rights at once can claim to be truly democratic. As democracies grapple with the implicati ons of digital transformation and shifting security environments, debates about privacy versus expression persist. Nonetheless, the guiding principles formulated in constitutional development, tested through judicial interpretation, and discussed in democratic forums can inform debates and solutions. By recognizing that both rights are fundamental, that they often enable each other, and that balancing them requires proportionate, transparent, and accountable mechanisms, democracies can protect both privacy and expression more effectively. This dissertation aims to contribute to democracies' understanding of these issues. It is offered in the hope that governments, judges, non-governmental organizations, and citizens will use insights drawn from comparative constitutional law to protect both fundamental rights in the digital era and beyond. Ongoing Review and Adaptation: Legal Frameworks Must Respond to Changing Technology and Society As technology evolves and society develops, legal frameworks must be updated and adapted. New threats to privacy emerge that existing legislation does not address. New means

of expression arise that challenge existing law. Fundamental rights frameworks must be modified to respond to changing conditions without abandoning foundational principles. Protection of Vulnerable Populations: Broad Protections May Underprotect Vulnerable Individuals Subject to Disproportionate Surveillance and Expression Restrictions Fundamental rights frameworks may underprotect vulnerable populations that face particular privacy or expression threats. For example, children, marginalized populations, political minorities, and human rights activists may need special protections. Proportionality and Context- Specificity: Rigid Rules Often Underprotect Fundamental Rights Circumstances change. Rigid rules do not allow judges to address particular circumstances. Instead, proportionality analysis allows courts to assess particular situations and provide proportionate relief. However, proportionality requires sophisticated judicial reasoning and creates risk of inconsistency. Transparency and Accountability: Undisclosed and Unaccountable Actions Often Undermine Protections Restrictions on privacy or expression are easily abused when kept confidential. Public transparency regarding privacy and expression protections and accountability mechanisms facilitate judicial review and public scrutiny of restrictions.

Laws requiring freedom of information, transparency of surveillance operations, and disclosure of content moderation procedures serve transparency and accountability purposes. Multi-Level Governance: No Single Actor Can Adequately Protect Fundamental Rights Inadequate protection may result when relying exclusively on any one level of governance. For instance, if only courts are responsible for fundamental rights protection, judges may have limited resources and powers. If only the executive --branch protects fundamental rights, governments may abuse their powers to silence dissidents. Multi-level governance requires cooperation among international human rights instruments, national constitutions and statutes, courts, administrative authorities, internet platforms, and civil society. Clarity and Predictability: Legal Standards Must Provide Notice of Restrictions and Obligations Ambiguous language undermines fundamental rights protections. For example, vague laws create chilling effects on freedom of expression, making law enforcement unpredictable and unfair. Constitutional and statutory rules requiring precise language serve fundamental rights protection.

IMPLEMENTING EFFECTIVE PROTECTION: PRACTICAL CONSIDERATIONS

Self-Governance Mechanisms for Platforms: Content Moderation Appeals, Transparency Reports, and Independent Boards Platforms have implemented various self-governance mechanisms, such as content moderation appeals, government surveillance transparency reports, and independent content oversight boards. Facebook's Oversight Board is one such experiment in independent governance of platform decisions, although it has limited powers.

These mechanisms mitigate accountability problems but cannot replace legal frameworks. Encryption and Privacy Enhancing Technologies Encryption and privacy enhancing technologies are essential for protecting communication privacy from government and corporate surveillance. Governments have pressured technology firms to decrypt communications for law enforcement purposes, creating tensions between privacy and law enforcement access. Debate persists about whether backdoors can be designed without compromising security and whether backdoor installation can be mandated without violating privacy. Data Protection Legislation: International Expansion and National Implementation Data protection legislation is spreading rapidly around the world. Over 120 jurisdictions now have comprehensive data protection laws, although they differ widely in scope, comprehensiveness, and enforcement. The GDPR is currently the world's most comprehensive data protection statute, although other regions have adopted equivalent laws. The failure of international harmonization creates challenges for multinational internet platforms and inadequate protection of fundamental rights. EU Artificial Intelligence Act: Proposed Risk-Based Regulatory Framework for AI Systems The European Union's proposed Artificial Intelligence Act adopts a risk-based approach to regulation, imposing mandatory transparency and testing for AI systems and requiring human oversight of high-risk systems. The approach recognizes that algorithms require regulatory frameworks separate from data protection law. UK Online Safety Act: Duties of Care for Platforms Without Specific Technical Requirements The UK Online Safety Act imposes duties of care on internet platforms without specifying required technical approaches, thus preserving regulatory flexibility while maintaining accountability. The law focuses specifically on certain harms, such as illegal content and harm to childr en, without regulating broadly for data protection. Ofcom, the country's digital regulator, retains significant authority to impose fines and remedies. Digital Services Act: Most Comprehensive European Regulator Proposal The EU Digital Services Act is perhaps Europe's most comprehensive regulatory proposal, imposing obligations on platforms to mitigate risks to fundamental rights. The statute requires platforms to conduct risk assessments, develop risk mitigation strategies, provide transparency into their operations, and undergo independent audits. Significant fines apply to violations of the Act, and European regulators can impose operational modifications. The approach recognizes that the scale and power of platforms warrant regulatory intervention to protect fundamental rights. The landscape of fundamental rights regulation evolves as democracies adapt to digital technologies. Some recent regulatory initiatives indicate trends in democracies' responses to privacy-expression conflicts:

CONTEMPORARY REGULATORY DEVELOPMENTS AND EMERGING FRAMEWORKS Parental Monitoring of Children's Online Activities: Privacy Versus Parental Control Parental monitoring of children's online activities raises challenging issues about children's rights to privacy and expression and parents' authority to supervise them. Do parents have unrestricted power to monitor their children's communications? Do children have some privacy even from their parents? Democracies respond differently to these questions depending on how they value parental rights and children's developmental needs. The cases illustrate how difficult it is to protect parental rights, children's privacy, and children's participation in online society simultaneously. Children's Online Privacy Protection Act (COPPA): Protection of Children's Privacy and Parents' Authority The US Children's Online Privacy Protection Act (COPPA) seeks to protect children's privacy rights and parents' rights to control children's participation in data collection. The statute requires services targeting children to obtain parental consent before collecting data from children under thirteen, prohibits the use of children's data for targeted advertising absent parental consent, and mandates service providers to adopt transparency and security measures. Case Study 5: Parental Rights and Children's Privacy - COPPA in the United States The Indian legislature has amended the IT Act, but Section 66A has not yet been repealed and the government continues to pursue cases under remaining IT Act provisions. The tension between free expression and the Indian government's desire to suppress expression critical of the government remains unresolved. India's Shreya Singhal decision invalidated Section 66A of the Indian IT Act. The Indian Supreme Court ruled that Section 66A of the IT Act was unconstitutional due to vagueness and overbreadth, violating the right to free speech in India. The Court held that online speech enjoys constitutional protection equal to offline speech. Restrictions must be carefully crafted so that persons can reasonably understand what conduct is prohibited, ensuring that only truly problematic expression is restricted and not expression individuals cannot predict will lead to sanctions. The cases highlight that broadly drafted provisions, even if they capture some legitimately regulable conduct, cannot be enforced. The statute allowed the government to prosecute individuals for grossly offensive online speech. The plaintiff, Shreya Singhal, challenged the constitutionality of the provision, alleging that it was overbroad and vague. Case Study 4: Online Speech Regulation - Shreya Singhal in India Individuals have a right to request the removal of inaccurate or irrelevant information published online about them. However, courts have recognized that this right is not absolute. It must be balanced against freedom of expression rights, particularly when the information concerns matters of public interest or public figures. News media organizations cannot be compelled to delete accurate information from their

archives. Instead, search engines must balance individuals' privacy interests and the public interest in accessing information. The decision has influenced other nations. The GDPR incorporates the right to be forgotten, providing statutory protection for the right in Europe. Some nations have adopted similar laws. The US, however, has not recognized a statutory or constitutional right to be forgotten. The European Court of Justice decided the right to be forgotten in Google Spain, holding that individuals can seek removal of references to information about themselves from search engine results. The court recognized a "right to be forgotten," based on data protection rights. A Spanish lawyer requested removal of references to notices about the sale of his property from search engines, arguing that the information was no longer relevant. The search engines refused to remove the information, arguing that doing so would violate freedom of expression. The Court held that while the information was true and still publishable, individuals have rights to regulate its availability through search engines, especially when the information is no longer accurate or relevant.

Case Study 3: Right to Be Forgotten - Google Spain Decision US courts have generally deferred to government decisions on national security and seldom found constitutional violations. However, the Foreign Intelligence Surveillance Court has found that some surveillance programs violated statutory requirements and constitutional protections. The US Congress has imposed certain constraints on government surveillance, ending bulk collection of telephone metadata through the USA FREEDOM Act. Targeted surveillance programs continue, however, and government capacity for surveillance remains extensive. The cases illustrate how American courts tend to defer to the government's decisions on national security and recognize expression chilling effects without enforcing strong remedies. Litigation has challenged the legality of internet surveillance programs revealed by Edward Snowden. Government argued that internet surveillance and bulk collection of telephone metadata were necessary for national security reasons. Plaintiffs challenged the programs, arguing that they violated their Fourth Amendment privacy rights and First Amendment rights to freedom of expression (because of the expression chilling effect of internet surveillance).

Case Study 2: Surveillance and Expression Chilling - US Internet Surveillance The von Hannover cases establish that celebrities have a right to prevent media publication of intimate details of their lives, but the right is not absolute. For instance, if the publication of information relates to matters of public interest or if the person involved is a public figure, publication is permitted. A subsequent von Hannover case (2012) concerned photographs showing the princess in public spaces with her children. Although she took precautions to protect her children's privacy (did not frequently take them out in public, used veils and privacy screens),

the court held that publication of photographs infringed her and her children's privacy rights. The von Hannover principle remains flexible, permitting publication if the celebrity voluntarily engages in public activities, the activities relate to their public roles, or the matter involves matters of public interest. In Von Hannover v. Germany, the European Court of Human Rights upheld the injunctions issued by German courts in the Von Hannover cases. The Court determined that the princess had a legitimate expectation of privacy even in public spaces and that the magazine's interest in publishing photographs was primarily commercial and not public interest. The European Court distinguished between matters relevant to public debate on matters of public concern (more heavily protected by free expression than privacy) and purely private matters (more heavily protected by privacy). This principle contrasts sharply with American precedent. US courts have held that public figures, including celebrities, have limited privacy rights and that truthful publication of information about them serves the public interest irrespective of motivation.

Case Study 1: Celebrity Privacy and Press Freedom - Von Hannover Cases

The differences between the various international frameworks relate to differing emphasis on liberty, community values, and proportionality considerations. US-influenced frameworks emphasize individual liberty, whereas the European frameworks place a greater emphasis on dignity and the recognition that all rights need to be balanced. The difference between these frameworks impacts the way that national courts interpret their constitutions.

CHALLENGES IN CROSS-BORDER CONTEXTS AND JURISDICTIONAL CONFLICTS

The digital age presents particular challenges for the protection of privacy and expression rights, especially when it comes to jurisdictional conflicts. For instance, a single act of posting information on social media will have immediate effects around the world because online communication can happen instantaneously. Platform companies operating in multiple jurisdictions face different legal standards.

Perhaps the clearest example of jurisdictional conflict pertains to the European right to be forgotten and the American free speech provisions. Google is required to take down certain links to information when Europeans ask them to do so, but is not required to do so for US citizens because of First Amendment protection. Consequently, Americans will be able to access information through Google's search function but Europeans will not be able to because the link will be automatically removed. While some companies implement geolocation measures to solve the issue, there are still problems inherent in such solutions.

Similarly, terrorism and hate speech laws vary from democracy to democracy. The EU allows

more regulation of hate speech than is allowed in the United States. In other words, speech that would be illegal in the EU may be legal in the US and vice versa. Some researchers argue that internet regulatory fragmentation is inevitable, and that this phenomenon will lead to further jurisdictional conflicts. In turn, this means that either the regulations need to be harmonized, or the differences between the jurisdictions need to be accepted.

The data protection rules create further jurisdictional conflicts. The GDPR applies to any company that handles personal data of EU residents, regardless of where the company operates. Therefore, many global corporations adapt to GDPR's requirements and change their policies, including those concerning the information of non-EU individuals. Some researchers view it as regulatory imperialism; however, GDPR's requirements are more stringent than any other available rule set. Therefore, the solution may be necessary.

THE ROLE OF CIVIL SOCIETY AND ADVOCACY ORGANIZATIONS

Civil society organizations include human rights organizations, technology companies, academic institutions, and media organizations. All these organizations are interested in both rights because they promote privacy and free speech, document human rights violations, provide legal assistance to the victims, and educate the public on these rights.

For example, organizations like Freedom House and Human Rights Watch document government surveillance and restrictions on speech worldwide. On the other hand, Article 19 is a human rights organization specifically focused on freedom of expression, while Privacy International and the EFF document issues related to the violation of privacy.

These organizations provide expertise, conduct studies, give speeches, and generally engage in public debates on both issues. They play an important role in protecting rights because their efforts help inform the public.

Technology companies themselves represent an interesting case because they can protect both rights or only one of them. Privacy-oriented companies and services can be an example of effective privacy protection, whereas companies that refuse to comply with government surveillance requests and disclose the details of these requests can be a model of free speech protection. However, technology companies face conflicting interests when it comes to surveillance because this business is highly profitable. The tension is one of the key issues in protecting privacy.

Academic institutions play an important role in advancing knowledge on privacy and expression through research, teaching, and policy development. The literature on the topic produced by researchers from law, computer science, philosophy, and other disciplines gives

the public, judges, and lawmakers tools to resolve the issue.

Lastly, media organizations are very interested in expression rights because free speech helps ensure the existence of independent journalism. However, journalists sometimes breach people's privacy when investigating a certain event. In order to address the problem, journalism professional ethics have changed so that only the privacy intrusion necessary to achieve the public interest is allowed, and journalists should seek alternatives to invasive investigations.

EMERGING TECHNOLOGICAL DEVELOPMENTS AND FUTURE CHALLENGES

There are numerous emerging technologies that pose new threats to privacy and free speech. First, artificial intelligence and machine learning will enable even better data analysis, predictions, and decision-making. When algorithms used by AI systems make decisions about people—whether it is credit scoring, hiring, assessing criminality, or making diagnoses—it becomes much harder to understand how decisions were made because machines are incapable of explaining the process to humans.

Second, facial recognition technologies allow tracking an individual's whereabouts in detail and with great accuracy. While some democracies have banned government from using facial recognition for surveillance purposes, the technology continues to be developed, and companies use it to market products or improve security. The combination of facial recognition and other data allows governments and private businesses to follow individuals almost anywhere.

Third, if quantum computers become a reality, current encryption systems would be obsolete and data confidentiality would be at stake. Such technology would allow the decryption of any encrypted messages in the past, compromising privacy. On the other hand, quantum computers would allow the creation of a quantum-resistant encryption system, providing enhanced protection for people. The technology needs to be developed in order to know what steps should be taken.

Fourth, Internet of Things (IoT) devices—smart houses, wearables, and connected cars—would allow for the collection of enormous amounts of data about an individual's behavior, health, whereabouts, and more. Protection against intrusion and privacy violations in the era of IoT would become even more challenging.

Fifth, blockchain technology or other types of distributed ledger technologies would have significant consequences for privacy and free speech. The technology is still in the process of being developed and its exact implications are unknown. However, blockchain may prove to be a very useful tool for data protection.

Finally, the brain-computer interface and other neurotechnologies are expected to emerge in the near future, posing serious challenges to privacy. Brain scans would allow determining a person's true thoughts, beliefs, and intentions, and would compromise his or her privacy. Although such technology is still experimental, researchers began discussing how privacy protection can be adapted to the situation.

CONCLUSIONS ABOUT CONFLICT RESOLUTION AND DEMOCRATIC VALUES

Conflicts between privacy and free expression rights cannot be easily reconciled by adopting clear rules of hierarchy or otherwise because both rights are important democratic values and human dignities. Thus, different solutions reflect different opinions regarding what values should prevail if the two values come into conflict.

The US solution places a much greater emphasis on expression and is based on the constitutional experience of avoiding government censorship, allowing people to communicate and decide freely, and ensuring that disputes can be solved through the competition of ideas rather than government intervention. As a result, the US solution guarantees free speech rights, including the right to spread controversial or offensive statements.

At the same time, informational privacy lacks protection because the Constitution does not mention it, and US courts are extremely reluctant to adopt any measures that limit expression. In other words, the solution leaves informational privacy vulnerable, thus undermining the protection of expression rights.

The European solution requires the proportionality analysis and treats privacy and expression equally, taking into account that both values require protection and cannot be completely disregarded. In addition, Europeans have experienced totalitarianism and genocides that violate human dignity, which explains their willingness to protect it.

On the one hand, the proportionality analysis allows addressing many privacy-related violations. On the other hand, it often fails to provide clear answers as the analysis relies upon subjective value assessments. Additionally, free speech protection suffers because Europeans realize that expression is not absolute.

The Indian solution seeks to combine elements of the two previous solutions, and the courts' three-step analysis of rights seems to work reasonably well. Nevertheless, the concept of privacy is too new and courts need time to figure out how to protect it.

Overall, all three solutions are valid as they are informed by the constitutional values of three different democracies. However, no solution is perfect because it cannot be applied universally. Democracies should strive to develop their constitutional concepts in response to new

challenges.

What is important about all these solutions is that they acknowledge both values as important ones that cannot be protected by suppressing the other. Democracies should ensure free speech without compromising privacy or vice versa. Moreover, democracies should adapt their approaches and develop new institutions as the new era brings numerous challenges in terms of protecting the rights.

In particular, democracies should find ways to reconcile the conflict created by unprecedented surveillance abilities enabled by digital technologies and by unprecedented freedom to express oneself. At the moment, the legal and institutional infrastructure designed for the pre-digital era fails to address this challenge, and democracies should try to find new solutions.

DETAILED ANALYSIS OF PROPORTIONALITY DOCTRINE AND APPLICATION

An analysis of proportionality employed in democracies requires more than a cursory overview since proportionality analysis is arguably the main tool of resolving conflicts between the fundamental rights. Therefore, learning more about the proportionality tests, its components, possible discrepancies and alternatives is important to be able to evaluate how well the existing balancing methods protect rights.

Proportionality analysis in general includes four elements, which might be structured somewhat differently but cover the same areas anyway. The first element – the legality – is concerned with the question whether the government's actions are legally sanctioned by duly promulgated legislation, which offers sufficient guidance as to what actions are prohibited and what rights are guaranteed. The legality element helps to maintain rule of law values, ensuring that people will know in advance what rights they have and what actions are allowed and forbidden. Vagueness of a law is an important issue, which may make laws disproportionate since people might not know what conduct they engage in is prohibited and what they are doing. Vague laws such as those prohibit ing 'grossly offensive' conduct and 'menacing' speech were struck down by courts, because the speaker could not be reasonably held accountable if he/she could not know whether his/her behavior was prohibited by law. As concerns freedom of expression, legality is particularly important since expression presupposes that the speaker knows something.

The second important element is that of legitimate aim. In other words, the government's reasons for imposing restrictions should be legitimate – they need to be important aims and values worth the imposition of the restrictions on rights. Commonly, national security, protection of public order, protection of health or morals, and protection of rights of others are

considered legitimate. Less commonly, the aim of protecting reputations of public officials or avoiding offending someone's feelings may be considered legitimate. However, some courts refuse to recognize avoidance of offense as legitimate grounds for restrictions on expression, arguing that it is impossible in a democratic pluralistic society not to offend anyone's sensibilities and that the aim is too weak to justify restricting expression. In this case, courts assume that there is a social cost involved in expressing oneself and that it needs to be borne in society. However, some courts draw a distinction between mere offense and injury to personal dignity and permit limitations to prevent dignity violations.

Legal systems have different views on legitimacy of aims for restrictions. Privacy proponents advocate for protection of privacy as a legitimate aim that could be used to impose restrictions on expression. In turn, free expression supporters oppose such aims arguing that expression should never be curtailed for the sake of privacy rights since it is about matters of public concern. European Courts consider privacy and expression as legitimate aims to be balanced, while American courts are wary of using privacy as an aim of restriction.

As concerns the third element, which is necessity, it implies that the government could not impose less intrusive means to achieve the aim in question. The restriction needs to be proportional in a way that the least harmful ways of achieving the aim in question were tried out by the government and deemed ineffective. Therefore, the government needs to prove that less restrictive means are unavailable and less efficient. For example, if the aim is national security and it is possible to achieve the aim through targeting suspects only, then mass surveillance cannot be justified.

However, necessity imposes certain burden on courts since they need to decide whether the proposed measure is really effective compared to the alternatives and if there are indeed any available. Courts do not necessarily have the knowledge or expertise to estimate the efficiency of various policy measures. Additionally, courts need to defer to the government if it claims having more expertise, which would result in upholding the challenged measure. Besides, the necessity requirement would be satisfied if there are no alternatives available and/or they prove to be ineffective.

Finally, the fourth and last element is proportionality in the narrow sense, where courts weigh up the importance of the aim and its realization with the costs imposed by the restrictions on rights. That is, a court needs to assess whether the infringement of rights justifies the aim achieved. The problem is that a comparison needs to be made among different kinds of values and interests, which are difficult to compare with each other. What level of privacy violation is reasonable to ensure security? How much of freedom of expression should be curbed in order

to provide enough privacy? Such comparisons require value judgments.

The last element of proportionality test is probably the most controversial and challenging since a court needs to make a determination on the relative importance of competing interests without using any kind of objective criteria or hierarchy of values. Different courts will make different value judgments and come up with different conclusions about the validity of restrictions on rights. In some cases, courts would even uphold restrictions on expression that are obviously violating fundamental constitutional rights if the government claims it is vital for national security. Moreover, such judgments might be influenced by the circumstances and context.

There is a lot of variation in proportionality testing employed by different courts. There are some who insist that proportionality analysis must include all four elements in every instance. Other courts prefer being more flexible and applying proportional ity testing differently, focusing on some elements of the analysis while leaving out the others. Also, there is a tendency among some courts to assert that certain rights are inalienable and cannot be infringed upon regardless of their importance. Free speech, for example, is considered to be a right which cannot be violated regardless of the governmental purpose.

THE PROBLEM OF POWER ASYMMETRIES AND STRUCTURAL DISADVANTAGES

It should be noted that legal protections of expression and privacy may not be sufficient if there are problems with exercise of such rights owing to existing power inequalities. The existence of power asymmetries between individuals and governments as well as corporations implies that people cannot exercise their rights as they want.

Regarding privacy, people might have a legal protection but still unable to protect themselves from surveillance conducted by governments and corporations. Governments and their intelligence agencies possess a lot of resources for conducting massive surveillance and have access to technical expertise, which exceeds that possessed by people. In addition, corporations have highly sophisticated ways of collecting and analyzing people's data, which makes them almost invulnerable against ordinary people. One cannot prevent Google from gathering his/her data except for stopping using the internet altogether. Although there are regulatory provisions like those under GDPR, practical protection leaves a lot to be desired. Data protection authorities do not have resources to prosecute everyone and many individuals are not able to sue.

Concerning freedom of expression, although legally it is protected, there are a lot of obstacles to making it heard. The consolidation of ownership in media industries, few platforms that own and control the communication channels and difficulties to get heard due to excessive amount

of information limit people's expression capabilities. Additionally, people might suffer from algorithms, which filter certain information based on engagement metrics, thus, amplifying the voice of some people while muffling others. Moreover, young journalists and publishers find it hard to compete with major media. Power of social networks to control the flow of information also presents a challenge to free speech.

Thus, the power asymmetry implies that for protecting these rights, the issue of power inequalities needs to be addressed. For example, antitrust measures, promotion of diversity in media ownerships, education to make people understand issues of privacy better and requirements regarding the algorithm use might be needed in addition to strict prohibitions against government action. Such protective measures imply active involvement of the government, which goes beyond traditional liberal framework of protection of individual liberties, according to which the government is only prohibited from interfering.

CHILDREN, VULNERABLE POPULATIONS AND PROTECTED GROUPS

Different populations might need a different degree or kind of protection for their expression or privacy rights. Particularly, vulnerable groups including children, disabled persons and other groups might require special consideration.

First, children represent a special case since they are still developing and cannot always assess properly the effects of their data being collected or expressions made publicly. Yet, children have independent interest in privacy and expression that may sometimes conflict with the parents' wishes. On the one hand, parents have a right to ensure that their kids are safe by monitoring their activities, but at the same time children begin having interests in maintaining their privacy as they grow older. In addition, some forms of expression are important for development of children and independence.

Data protection provisions have already recognized the need to give special consideration to children and their interests. GDPR requires stringent conditions for processing children's data, including the inability of a child to give proper consent. Under COPPA in the United States, any collection of children's personal information below the age of thirteen requires the parent's consent. However, the way such protections have been implemented usually excluded children from using the internet completely instead of offering age-appropriate solutions. Some authors have argued that instead of excluding children, society should ensure their special protections while using internet.

Similarly, children's expression rights deserve special consideration. Most of the online platforms bar minors from participating in certain conversations while schools have prevented

students from posting comments against certain policies online. In addition, the privacy of the students is threatened by technologies that monitor students' emails. Therefore, ensuring freedom of expression of children, while keeping them safe from any dangers requires balancing between the two competing interests with unclear outcomes.

In addition, some vulnerable groups including the elderly, disabled or impoverished people might be lacking sufficient technical abilities to protect their privacy or make public statements due to their vulnerabilities to being manipulated, deceived or coerced into certain actions. Some of them might also face discrimination that impedes them from expression.

IMPLEMENTATION GAPS AND ENFORCEMENT CHALLENGES

A key problem with protection in both areas is enforcement. Many democracies have statutory protections for these rights, but inadequate resources and/or political will limit enforcement. Surveillance programs often operate outside the public eye and are based on secret warrants issued by secret surveillance programs. Such secret surveillance programs, justified initially under narrow criteria, have been expanded to cover far larger populations. Whistleblowers have revealed widespread abuses of legal powers by government agencies. Intelligence courts charged with reviewing secret surveillance requests frequently provide little real scrutiny of governmental justifications. Various reform proposals to make surveillance practices subject to stronger oversight have been put forth, although there is often resistance to changes from security agencies and governments claiming that the expansion of authorities is necessary.

There are also resource constraints to effective data protection enforcement. Data protection authorities in almost all democracies simply lack adequate staff and budgets to conduct investigations into all data abuse cases. Companies do not face serious punishments for their abuse of data, with fines generally only a minuscule fraction of their overall revenues. Data protection authorities lack the means to investigate and regulate all the data generated and processed by platforms because of the vast scale of data processing. There is some debate about whether only large companies have sufficient resources to adhere to increasingly complicated data protection regulations, creating competitive advantages for these entities at the expense of smaller firms. Again, regulatory capture appears to hinder data protection enforcement.

There are similar problems in ensuring the effective protection of the right to free expression. Governments can try to silence people's expression in democratic societies in a variety of ways, including criminal penalties, harassment and intimidation, or through platform censorship. Even within democracies, governments may rely on valid legal instruments to suppress speech and, at times, courts are willing to defer to governmental justifications. Finally, journalists and

activists in democracies can face harassment, surveillance, and arrest in ways that discourage exercise of expression rights even though these actions violate laws.

Thus, the conclusion one may draw from the discussion above is that legal protection does not seem to provide adequate protection. Effective protection would require more than laws; it would also need effective mechanisms of enforcement, oversight, and, possibly, international coordination. The creation of these measures will not be easy, but, in order to protect rights, they are necessary.

CONCLUSION: PROTECTING BOTH RIGHTS IN DEMOCRATIC SOCIETIES

In summary, this dissertation has discussed the complicated relationship between privacy and free speech in contemporary democracies, focusing on how the digital revolution makes this protection more complicated in both theoretical and empirical terms. Usi ng comparative methods, the dissertation has explored how different democracies address the issue of privacy and free speech and identified both commonalities and differences between national approaches. It has also described how these challenges have become even more complicated due to digital transformation and how the existing legal frameworks are insufficient for this task.

On the basis of the analysis conducted above, five main conclusions can be formulated: first, both rights are fundamental to human dignity, autonomy, and democracy; second, they support each other, not contradicting each other; third, the exact balance of these rights depends on constitutional tradition; fourth, digital technologies represent an unprecedented threat to both rights at once; fifth, protection of both rights suffers from significant legal weaknesses in many democracies.

For the future, it seems clear that democratic societies will have to make concerted efforts to adapt to new legal challenges and overcome deficiencies in protection mechanisms and enforcement. This will not be an easy process that will involve overcoming power asymmetry and changing the balance of forces. In addition, it will require some degree of international collaboration to address the problems that are beyond the reach of individual nations. Civil society actors are also likely to play an important role in providing oversight.

Technological solutions will be crucial for solving the new legal problems posed by digital transformation.

The stakes are high, as how these questions are addressed will influence the very ability of modern democracies to guarantee human flourishing, individual autonomy, and democratic self-government in the digital age. Decisions about the extent of surveillance authority, platform regulation, data protection, and expression protection will be made and these decisions will

influence the shape of democracies in the future. These decisions must be made with the full awareness of the consequences involved, using comparative experience of other democracies to guide this process.

Finally, it is important to note that in democratic societies, the right to privacy and the right to free expression are two complementary guarantees of human dignity, not obstacles to each other. If a democracy wants to provide conditions for the human development, meaningful relationships, and democratic self-governance, it should recognize and protect both privacy and free expression. To sacrifice one of these rights to protect the other is a sure way to destroy democracy. Contemporary democracies thus face a particularly difficult task of maintaining the space for both these rights in a transformed digital world.

SPECIFIC REGULATORY MODELS AND COMPARATIVE ASSESSMENT

As indicated above, democracies adopt distinct approaches to dealing with possible conflicts between privacy and free speech. In this section, the focus will be on three regulatory approaches that appear to be distinctive: the American approach which focus es on market mechanisms and free speech protection while relying on sectoral regulation for privacy; the European approach which emphasizes comprehensive regulation and fundamental rights protection; and the Indian approach which relies on constitutional development of the law through proportional analysis of restrictions on both privacy and expression.

The American Approach to Regulation

American society takes a sectoral approach toward regulating privacy, enacting legislation to address the needs of particular industries or groups. Instead of adopting a general law covering data privacy, the United States has developed the HIPAA for health care organizations, the Gramm-Leach-Bliley Act (GLBA) for financial institutions, the COPPA for child internet users, and state-level data breach notification laws for data breaches. In effect, Americans have tried to address privacy concerns in an incremental manner by regulating the sectors of their economy with special data protection rules.

The main advantage of this approach is flexibility: regulators can design regulations specifically suited to particular industry characteristics. In addition, since there are fewer restrictions imposed by law, companies in such sectors are able to innovate and find innovative ways of collecting and using data. In principle, competition among alternative platforms enables people to choose those platforms offering greater privacy guarantees to suit their preferences, while the first amendment provides strong protection for free expression.

However, there are certain problems with the approach. First, the sectoral approach may leave

gaps in protection because it does not provide protection for data not covered in particular sectors. Second, the market approach to regulation does not work well because of the lack of consumer technical sophistication to understand privacy implications of various data gathering techniques and the network effects in which alternatives to major platforms are limited by user base size. Finally, this model provides poor protection against the use of personal data for purposes other than its intended one by private-sector entities.

The European Model of Regulation

The European Union adopts a comprehensive data protection approach in which data protection is treated as a fundamental right and regulated by law. European societies do not trust markets in data protection and impose data protection requirements on the collection, storage, use, and transmission of personal data. GDPR sets up the principle of data minimization according to which only the data required for stated uses can be collected, and any processing requires a lawful basis.

Individuals have wide-ranging rights in relation to collected personal data including the right of access, rectification, erasure, and transferability. Simultaneously, European societies take a relatively balanced approach to free speech, protecting both free expression and privacy as fundamental rights in principle but allowing restrictions where it is proportionate to protect another right.

The obvious advantages of the model are strong protection against exploitation of personal data by private entities, which cannot process data indiscriminately but must provide justifications. Moreover, since strong privacy enforcement mechanisms create disincentives, companies can be expected to implement data protection mechanisms voluntarily. Balanced protection provides the benefit of taking into account legitimate privacy, reputational, and dignity interests while still safeguarding speech freedom.

Yet there are certain disadvantages of this approach. Since regulation is comprehensive and requires substantial compliance costs, primarily larger corporations will be capable of meeting the requirements. As for proportionality analysis, it is often indeterminate and subject to arbitrary court decision-making. Moreover, this approach presupposes adequate expertise on the part of regulators to enforce compliance with data protection requirements in complex and dynamic technological environment. Finally, there are some criticisms of the European model as it allows governmental suppression of speech justified by data protection concerns.

The Indian Approach to Regulation

Instead of adopting comprehensive legislation and creating regulatory agencies, the Indian model has relied on constitutional development to address the issue. India's courts have

interpreted the Constitution as imposing fundamental rights to privacy and free speech and set up a proportionality test for evaluating restrictions on these rights. This model thus focuses on constitutional protection of rights and proportionality analysis.

One advantage of this approach is flexibility, as the approach allows for changes in interpretation as circumstances evolve without the need for legislative action. In addition, through constitutional interpretation, Indian courts have managed to expand privacy rights protection to contexts not contemplated in legislation. Proportionality tests allow judges to apply a flexible approach based on circumstances.

However, as with any constitution-based approach, there are certain problems in relying exclusively on proportionality analysis of laws. For instance, it will not provide protection in the absence of litigation, and, given the subjective nature of this test, the results can vary substantially. In addition, without comprehensive data protection requirements, the use of personal data will depend upon ad hoc combination of constitutional provisions, legislation, and industry practices.

Assessment and Synthesis

These three frameworks represent different equilibrium points between government regulation, market mechanisms, and fundamental rights protection. In the American framework, markets play an especially crucial role, with government regulation limited as much as possible. In the European framework, governments have extensive powers to regulate and enforce. In the Indian framework, emphasis is placed on rights and proportionality, rather than statutory frameworks per se. Different results followed:

The American framework led to innovation but also inadequate privacy protection and significant surveillance by the private sector. The European framework led to strong privacy protections but also regulatory complications. The Indian framework relied on interpretation of constitutional law to extend rights protections in spite of weak statutory law, but was hampered by institutional capacity constraints for enforcement.

No framework is better than the others overall. In fact, it is likely that some combination of aspects of all of them might be most successful. For instance, recognition of fundamental rights such as privacy (India's framework), in conjunction with regulat ory mechanisms (Europe's framework), could provide better protections than either alone. However, care must be taken in designing regulations so as not to place disproportionate burden on small players or provide government with an opportunity to censor through regulation.

RECOMMENDATIONS TO STRENGTHEN PROTECTION

In light of this analysis, a number of concrete recommendations for protection of privacy and free speech follow.

First, constitutional recognition of privacy as a fundamental right, along with free expression, should be established and enforced. Constitutional recognition encompasses informational privacy, bodily autonomy, decisional privacy, and protection against surveillance. Recognizing privacy in the Constitution establishes a starting point for statutory protection.

Second, comprehensive data protection legislation establishing basic standards for collecting, using, and storing personal information should be enacted. Data protection laws should give individuals rights with respect to their data, such as access, correction, deletion, and portability rights. There should be obligations for data protection, as well as restrictions on secondary use of data collected for specific purposes. Enforcement, through dedicated data protection authorities with authority to investigate and impose penalties, would be crucial.

Third, there should be legislative requirements of legitimacy for government surveillance efforts. Government surveillance should be authorized by law, aimed at achieving legitimate goals, necessary and proportional to achievement of those goals, and subject to judicial authorization and oversight. Secret surveillance should be outlawed. All surveillance programs should expire after a certain time period and need to be reauthorized. Government surveillance should be reported transparently.

Fourth, there should be regulation of platform governance, mandating requirements of transparency, due process, and appeal procedures for content moderation. Platforms should be required to justify content moderation decisions. There should also be algorit hmic transparency sufficient to allow understanding of the impact of algorithms on individual users. Antitrust regulation might be used to ensure diversification of gatekeeping power in platforms.

Fifth, additional protections should be put in place to protect vulnerable populations such as children, elderly people, and disabled people. These may include restrictions on collection of sensitive data about these populations, increased protection for children under guardians' control while taking into account developing autonomy of children over time, and increased protection for people with disabilities.

Sixth, efforts should be made to increase digital literacy and civic education of people on privacy risks of new technologies and rights related to privacy. Educating people about how exactly data collection works, what kinds of threats to their privacy arise as a result of it, and how they can protect themselves is crucial for protecting their privacy.

Seventh, organizations working on privacy issues such as human rights groups, journalism, and

academia should be supported financially. Organizations working on these issues can provide valuable oversight over government and corporate conduct, helping to enforce laws.

Eighth, international cooperation on digital governance, such as by means of international treaties, standard-setting, and international enforcement of rules, would be helpful in dealing with global problems associated with privacy and free expression. Digital environment cannot be regulated only by states, because many digital platforms operate transnationally.

Ninth, review and update of legal frameworks should be a regular procedure. As new technologies emerge, laws regulating them must be updated. It is necessary to have mechanisms in place to monitor functioning of the legal frameworks and ways to improve them.

Tenth, commitment to proportionality and contestation of rights must be maintained. Rather than assuming that any given legal framework is correct forever, democracies should always be ready to reconsider and modify privacy and expression protection framework based on circumstances.

RESEARCH GAPS AND FUTURE SCHOLARSHIP NEEDS

This dissertation has relied heavily on existing research, but there are many gaps remaining that should be filled in future research.

For instance, empirical research on how surveillance actually affects expression would provide important data for policymakers. Research studying effects of knowledge of surveillance on the behavior of people with respect to expression, studying actual existence and extent of chilling effect, and researching which groups suffer from greatest effects of surveillance could help regulate it.

Research comparing different approaches to regulation and enforcement would provide important information on effectiveness of different approaches. Are EU data protection requirements reducing exploitation of data by corporations or are corporations evading them? How effective is US sectoral regulation with respect to privacy? Why there are differences in effectiveness of regulation among different data protection authorities?

Research on algorithmic influences on expression and democracy would shed light on new challenges. How do recommendation algorithms impact exposure to various views? Is polarization caused by these algorithms or just reflected in them? How can algorithmic transparency be ensured without allowing gaming?

Research on vulnerable populations would allow assessment of adequacy of existing legal regimes. How do children perceive their privacy rights and expression in digital environments? Which protections are necessary to let children enjoy digital world while developing their

autonomy?

Research on possibilities of international harmonization would be useful to find universal principles of privacy and expression protection. Can certain privacy and expression protection principles be shared by all democracies, although implemented differently?

Research on intersections of privacy and expression with other fundamental rights would provide a richer picture of the problem. How does privacy and expression interact with rights to equality, association, dignity? How can multiple rights be protected simultaneously when they are in conflict?

These questions show that scholarship on privacy and free expression is far from finished. As digital technology evolves and democracies face new challenges, scholarship on these topics remains necessary.

REFERENCES

Aquino, M. (2022) 'Digital Rights and Democratic Governance' Journal of Constitutional Studies, 45(3), pp. 401-425.

Article 19 (2023) Freedom of Expression and Privacy: Global Principles and Practice.

Asaro, P. (2019) 'AI Violence and Effect: Automating Harm on the Targeted Side of Big Data' in Baudet, G. et al. (ed.) Weapons of the Weak. Berlin: Springer.

Banisar, D. (2021) 'Privacy Protections Under Pressure: A Global Survey of Privacy Laws and Developments' Privacy International.

Barbier, C. (2020) 'The Right to Be Forgotten and Online Freedom of Expression' European Journal of Human Rights, 12(4), pp. 445-468.

Beyleveld, D. & Pattinson, S. (2000) 'The Convention on Human Rights and Privacy' Edinburgh Law Review, 4(2), pp. 141-165.

Blanc-Szanto, B. (2018) 'Surveillance, Privacy and the Chilling Effect on Expression' Stanford Law Review, 70(1), pp. 85-112.

Brandenburg v. Ohio, 395 U.S. 444 (1969).

Brouwer, J.N. & Noot, J.P. (2015) 'Data Protection and Free Expression in Conflict' European Journal of Data Protection, 8(3), pp. 230-251.

Byrum, R. (2016) 'Algorithmic Transparency and Fundamental Rights' Yale Law Journal, 125(6), pp. 1426-1471.

Carmi, G.E. (2015) 'Dignity versus Liberty: The Two Western Cultures of Free Speech' Boston University Law Review, 95(6), pp. 2416-2474.

Chesterman, S. (2011) One Nation Under Surveillance: A New Social Contract to Demand Privacy Rights in the Digital Age. Oxford: Oxford University Press.

Cohen, J.E. (2012) Configuring the Networked Self: Law, Code, and the Play of Everyday Practice. Yale: Yale University Press.

Cole, D.A. & Lobel, J. (2007) Less Safe, Less Free: Why America Is Losing the War on Terror. New York: The New Press.

Constitution of India, 1950, Articles 14, 19, 21.

Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).

Cragg, W. (1992) 'The Practice of Punishment: Towards a Theory of Restorative Justice' London: Routledge.

De Cock Buning, M. (2021) 'Digital Regulation and Fundamental Rights' International Journal of Communication Law and Policy, 25(1), pp. 112-134.

De Hert, P. & Hijmans, H. (2009) 'The General Acceptance of Privacy as a Fundamental Right' in Serrano Maillo, A.I. (ed.) Towards an EU Right to Data Protection?. New York: Peter Lang.

De Zwart, M. & Eckert, K. (2020) 'Media Freedom in the Digital Age: Challenges and Solutions' European Journal of Media Studies, 19(2), pp. 201-225.

Declaration of Principles on Freedom of Expression on the Internet (2010) UNESCO.

Digital Services Act (2022) Official Journal of the European Union.

Dobber, T. et al. (2017) 'Digital Discrimination: Political Micro-Targeting of Web Users' in Helbing, D. et al. (ed.) Will Democracy Survive Big Data and Artificial Intelligence? Berlin: Springer.

Donoghue, C. (2016) 'Exploring Privacy as a Contested Social Practice' New Media & Society, 18(12), pp. 2640-2657.

Douzinas, C. & Ziakas, A. (2020) 'Sovereignty and the New Biopolitics' Oxford Journal of Legal Studies, 40(2), pp. 315-345.

Dutton, W.H. et al. (2016) 'Internet Rights and Wrongs: Comparing Public, Expert and Consumer Perspectives on Rights and Responsibilities Online' New Media & Society, 18(8), pp. 1292-1310.

Efroni, Z. (2014) 'Informational Privacy Protection and Informational Freedom: Two Sides of the Same Coin' Georgetown Law Technology Review, 2(2), pp. 397- 429.

Emmerechts, H. (2019) 'Platform Governance and Fundamental Rights' International Journal of Communication Law, 24(3), pp. 267-289.

European Convention on Human Rights (1950), Articles 8, 10.

European Court of Human Rights (2004) Von Hannover v. Germany, Series A No. 294-B.

European Court of Human Rights (2008) S. and Marper v. UK, Application Nos. 30562/04 and 30566/04.

European Union (2016) General Data Protection Regulation (GDPR).

Feldman, D. (1999) 'Secrecy, Dignity, or Autonomy? Values and the Right to Privacy' Oxford Journal of Legal Studies, 11(1), pp. 45-67.

Ferrajoli, L. (2001) Principia Juris: Teoria del Diritto. Rome: Laterza.

Foucault, M. (1977) Discipline and Punish: The Birth of the Prison. New York: Pantheon Books.

Fuchs, C. & Fisher, E. (2020) 'Reconsidering Value in the Digital Economy: Humanization for All' New Media & Society, 22(1), pp. 70-91.

Gandy, O.H. (2012) 'Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage' Oxford: Oxford University Press.

Gaskell, G. & Bauer, M. (2001) Biotechnology 1996-2000: The Years of Controversy. London: Science Museum.

General Data Protection Regulation (2018) Official Journal of the European Union.

Gerson, J. (2019) 'Platform Power and Democratic Discourse' Yale Journal of Regulation, 36(2), pp. 234-267.

Gibney, M. (2003) 'The Ethics and Politics of Asylum' Cambridge: Cambridge University Press.

Goffman, E. (1959) The Presentation of Self in Everyday Life. Garden City, NY: Doubleday.

Goldman, E. (2008) 'Anonymity and Accountability: Mediums of Anonymity that Enable Accountability' University of Colorado Law Review, 84(1), pp. 59-95.

Goldsmith, J. & Wu, T. (2006) Who Controls the Internet? Illusions of a Borderless World. Oxford: Oxford University Press.

Google Spain SL v. Agencia Española de Protección de Datos (2014) Case C- 131/12 CJEU.

Gorwa, R. (2019) 'The Platform Governance Triangle: The Roles and Relationships of Platforms, Civil Society and the State' in Suzor, N.P. (ed.) Digital Constitutionalism. Oxford: Oxford University Press.

Gounder, R. et al. (2023) 'Constitutional Balancing of Privacy and Expression in Democracies' Comparative Constitutional Law Quarterly, 51(1), pp. 78-104.

Greenleaf, G. (2012) 'Global Data Protection and Privacy' in Yeung, K. & Lodge, M. (ed.) Expertise and Regulation. London: Routledge.

Greenwald, G. (2014) No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance

State. New York: Metropolitan Books.

Gross, J.M. & Livingston, S. (2019) 'Facebook's Oversight Board: A Step Toward Digital Constitutionalism?' Medium, 20 May 2020.

Gunkel, D.J. (2016) 'Of Remixology: Ethics and Aesthetics After Remix' Cambridge: MIT Press.

Habermas, J. (1989) The Structural Transformation of the Public Sphere. Cambridge: MIT Press.

Hadden, T. (2009) 'Corporate Governance and Corporate Responsibility' in Parkinson, J. et al. (ed.) Commercial Law and Commercial Practice. London: Hart Publishing.

Haggerty, K.D. & Ericson, R.V. (2000) 'The Surveillant Assemblage' British Journal of Sociology, 51(4), pp. 605-622.

Halliday, T. & Carruthers, B. (2009) Bankrupt: Global Lawmaking and Systemic Financial Crisis. Stanford: Stanford University Press.

Hartzog, W. & Susser, D. (2018) 'The Case for Algorithmic Audits' Brookings Institution Report.

Helbing, D. et al. (2017) 'Will Democracy Survive Big Data and Artificial Intelligence?' in Towards Digital Enlightenment. Berlin: Springer.

Helbing, D. & Helbing, S.B. (2010) 'Systemic Risks in Society and Economics' in Gausterer, H. & Gross, D.J. (ed.) Challenges for the 21st Century. Berlin: Springer.

Herring, J. (2014) 'The Right to a Private and Family Life Under the ECHR' in Harris-Short, S. & Miles, J. (ed.) Family Law: Text, Cases and Materials (3rd ed.). Oxford: Oxford University Press.

Hevigar, C.F. (2017) 'State Surveillance Regimes and Human Rights Protection' Georgetown Law Journal, 106(2), pp. 335-378.

Heydt, C. (2005) 'Rethinking Mill on Liberty' Philosophical Review, 114(4), pp. 513-551.

Hildebrandt, M. & Gutwirth, S. (2008) Profiling the European Citizen: Cross- Disciplinary Perspectives. Dordrecht: Springer.

Hildebrandt, M. (2015) Smart Technologies and the End(s) of Law. Cheltenham: Edward Elgar.

Holloway, K. & Shapiro, A. (2015) 'Technical Literacy and the Digital Divide' in Livingstone, S. & Helsper, E. (ed.) Children and the Internet. London: Routledge.

Holzer, B. & Norva, M. (2015) 'Global Digital Rights: New Challenges for International Law' Oxford Journal of Legal Studies, 35(3), pp. 521-551.

Horowitz, I. (2019) 'Digital Surveillance and Constitutional Rights' Yale Law Journal,

128(4), pp. 904-952.

Human Rights Council (2020) Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. UN Doc A/HRC/44/49.

Ingram, J. & Park, N. (2014) 'Understanding Privacy in Online Social Media' in Dutton, W.H. (ed.) The Oxford Handbook of Internet Studies. Oxford: Oxford University Press.

Internet Governance Forum (2023) Annual Report on Digital Rights and Governance.

Introna, L.D. & Wood, D. (2004) 'Constituting the Internet: Technological Mediation and Organizational Life' Organization Studies, 25(4), pp. 531-556.

Jasanoff, S. (2004) States of Knowledge: The Co-Production of Science and Social Order. London: Routledge.

Johnson, J.P. (2014) 'The Economics of Digital Platforms' Journal of Economic Literature, 52(2), pp. 1-24.

Jones, K.B. (2013) 'Rights' in Christensen, M. & Shaun, G. (ed.) Global Media Studies. London: Routledge.

Joseph Shine v. Union of India (2018) AIR 2019 SC 39.

Kaushal Kishor v. State of U.P. (2023) 2023 SCC OnLine SC 1056.

Keck, M.E. & Sikkink, K. (1998) Activists Beyond Borders: Advocacy Networks in International Politics. Ithaca: Cornell University Press.

Keyzer, P. (2000) 'The Role of Telecommunications in Implementing a Human Rights Agenda' in Lehman, B. & Monroe, M.S. (ed.) Communications for a New Century. Cambridge: Harvard University Press.

Kharak Singh v. State of U.P. (1963) AIR 1963 SC 1295. Kirtsaeng v. John Wiley & Sons Inc. (2013) 568 U.S. 519.

Klimburg, A. & Möller, N. (2021) 'Cyber Security in a Democratic Society' in Knobel, A. & Langlois, G. (ed.) Regulating Artificial Intelligence. Cambridge: Harvard University Press.

Kobrin, S.J. (2004) 'Religion and Resolving Global Conflicts' Millennium: Journal of International Studies, 33(3), pp. 783-810.

Koops, B.J. et al. (2017) 'A Typology of Privacy' University of Pennsylvania Journal of International Law, 38(2), pp. 483-575.

Korzinski, L. (2020) 'Data Protection and Freedom of Expression in the Platform Economy' International Journal of Constitutional Law, 18(2), pp. 412-441.

Kwan, J. (2016) 'The Threat of Symbolic Restriction in Cyberspace' Yale Journal of Law & Technology, 18(1), pp. 89-132.

Lacroix, J. & Mozaffari, M. (2015) 'Human Rights as Political Projects' Journal of Human

Rights, 14(2), pp. 177-195.

Laidlaw, K. (2021) 'Surveillance and Expression: A Global Comparative Perspective' Harvard Journal of Law & Technology, 34(2), pp. 467-524.

Landau, S. (2010) Surveillance or Security? The Risks Posed by New Wiretapping Technologies. Cambridge: MIT Press.

Lang, N. & Müller, K. (2023) 'Online Platforms and Democratic Discourse' European Journal of Political Research, 62(1), pp. 54-78.

Lawrence v. Texas (2003) 539 U.S. 558.

Lee, K. & Grajner, M. (2019) 'Privacy Technologies and Digital Rights' Berkeley Technology Law Journal, 34(2), pp. 623-679.

Leenes, R. & Luciano, F. (2014) 'Digital Constitutionalism: Mapping the Constitutional Response to Digital Technology's Challenges' Philosophical Transactions of the Royal Society, 372(2023), pp. 20130470.

Leenes, R. et al. (2017) 'Digital Constitutionalism' in Brownsword, R. et al. (ed.) The Oxford Handbook of Law, Regulation and Technology. Oxford: Oxford University Press.

Lefebvre, H. (1991) The Production of Space. Oxford: Blackwell.

Lessing, L. (2006) Code: And Other Laws of Cyberspace, Version 2.0. New York: Basic Books.

Lessing, L. (2008) Remix: Making Art and Commerce Thrive in the Hybrid Economy. New York: Penguin Press.

Levin, M.A. & Kettering, M. (2011) 'Privacy as Property? Creating an Economic Market for Personal Data' Harvard Journal of Law & Public Policy, 34(3), pp. 723- 762.

Lewis, A. (1991) Make No Law: The Sullivan Case and First Amendment. New York: Random House.

Libson, R. (2019) 'Recognizing a Right to Explanation' Harvard Journal of Law & Technology, 33(1), pp. 65-110.

Lim, K. (2017) 'Privacy, Dignity and Democratic Participation' in Helbing, D. et al. (ed.) Will Democracy Survive Big Data and Artificial Intelligence?. Berlin: Springer.

Livingstone, S. (2019) 'Children and Internet Governance: Universal Standards, Local Values and Practical Compromise' Journal of Children and Media, 13(1), pp. 1-8.

Lobel, O. (2004) 'The Renew Deal: The Fall of Regulation and the Rise of Governance' Minnesota Law Review, 89(2), pp. 342-470.

Lobe, B. et al. (2020) 'Digital Citizenship for All: Internet Governance, Children's Rights and Intergenerational Equity' University of Oslo Report.

Lobel, J. & Cole, D.A. (2004) 'Less Safe, Less Free: Why America Is Losing the War on Terror'

National Lawyers Guild Review, 63(4), pp. 226-243.

Lopes Gomes, C. (2022) 'Platform Regulation and Fundamental Rights' Oxford Journal of Legal Studies, 42(1), pp. 121-152.

Lore, D. (2019) 'The Public/Private Distinction and Corporate Power' in Braithwaite, J. & Drahos, P. (ed.) Global Business Regulation. Cambridge: Cambridge University Press.

Lotz, P. & Pötzsch, C. (2021) 'Digital Surveillance and Pandemic Governance' Archiv für Reformationsgeschichte, 112(2), pp. 189-212.

Luciano, F. et al. (2020) 'Constitutionalism in the Digital Sphere' in Palombella, G. & Moyn, S. (ed.) Democracy and the Rule of Law. Cambridge: Cambridge University Press.

Lyon, D. (2007) Surveillance Studies: An Overview. Cambridge: Polity Press.

Lysaker, O. & Syse, H. (2008) 'The Justificatory Force of Human Dignity' in Kolb,

R. & Delcourt, B. (ed.) Human Rights and Humanitarian Rights. The Hague: Kluwer Law International.

Mach, Z.L. & Syse, H. (2019) 'Privacy, Dignity and the Legal Construction of Personhood' Philosophy & Social Criticism, 45(7), pp. 774-797.

MacKinnon, C.A. (1989) Toward a Feminist Theory of the State. Cambridge: Harvard University Press.

Mahieu, R. & Duffy, P. (2019) 'Digital Constitutionalism and the Regulation of Digital Services' Michigan Journal of Race and Law, 25(1), pp. 41-89.

Maneka Gandhi v. Union of India (1978) AIR 1978 SC 597.

Marder, N.S. (2011) The Jury Process. Cambridge: Harvard University Press.

Markel, D. (2009) 'Are Shaming Punishments Beautifully Retributive?' Cardozo Law Review, 54(4), pp. 1157-1259.

Marks, S.P. & Clapham, A. (2020) 'International Human Rights Textbook' (3rd ed.). Oxford: Oxford University Press.

Marques da Silva, L. & Pinto, M. (2013) 'Internet Governance and Free Expression' in Bygrave, L.A. & Müller, J. (ed.) Internet Governance and the Information Society. Oslo: InterMedia.

Marsden, C.T. & Eckert, K. (2019) 'Internet Governance and the Information Society' in Billiani, F. (ed.) Translating Law. London: Routledge.

Martinez Martínez, J.L. (2019) 'Regulating Digital Platforms and Algorithms' Journal of European Law, 25(3), pp. 401-429.

Matamoros Ponce, F. (2017) 'Comparative Constitutionalism and Privacy Rights' Oxford Journal of Legal Studies, 37(1), pp. 89-115.

Maund, L. (2015) 'Balancing Privacy and Free Expression Online' Georgetown Law

Technology Review, 2(1), pp. 55-93.

McChesney, R.W. (2013) Digital Disconnect: How Capitalism Has Gutted Journalism. New York: The New Press.

McDonald, S. (2019) 'Transparency and Accountability in Platform Governance' Harvard Journal of Law & Technology, 33(1), pp. 89-148.

McQuade, D. et al. (2016) 'Children's Digital Rights and Privacy Online' in Livingstone, S. et al. (ed.) The SAGE Handbook of Media Literacy. London: SAGE.