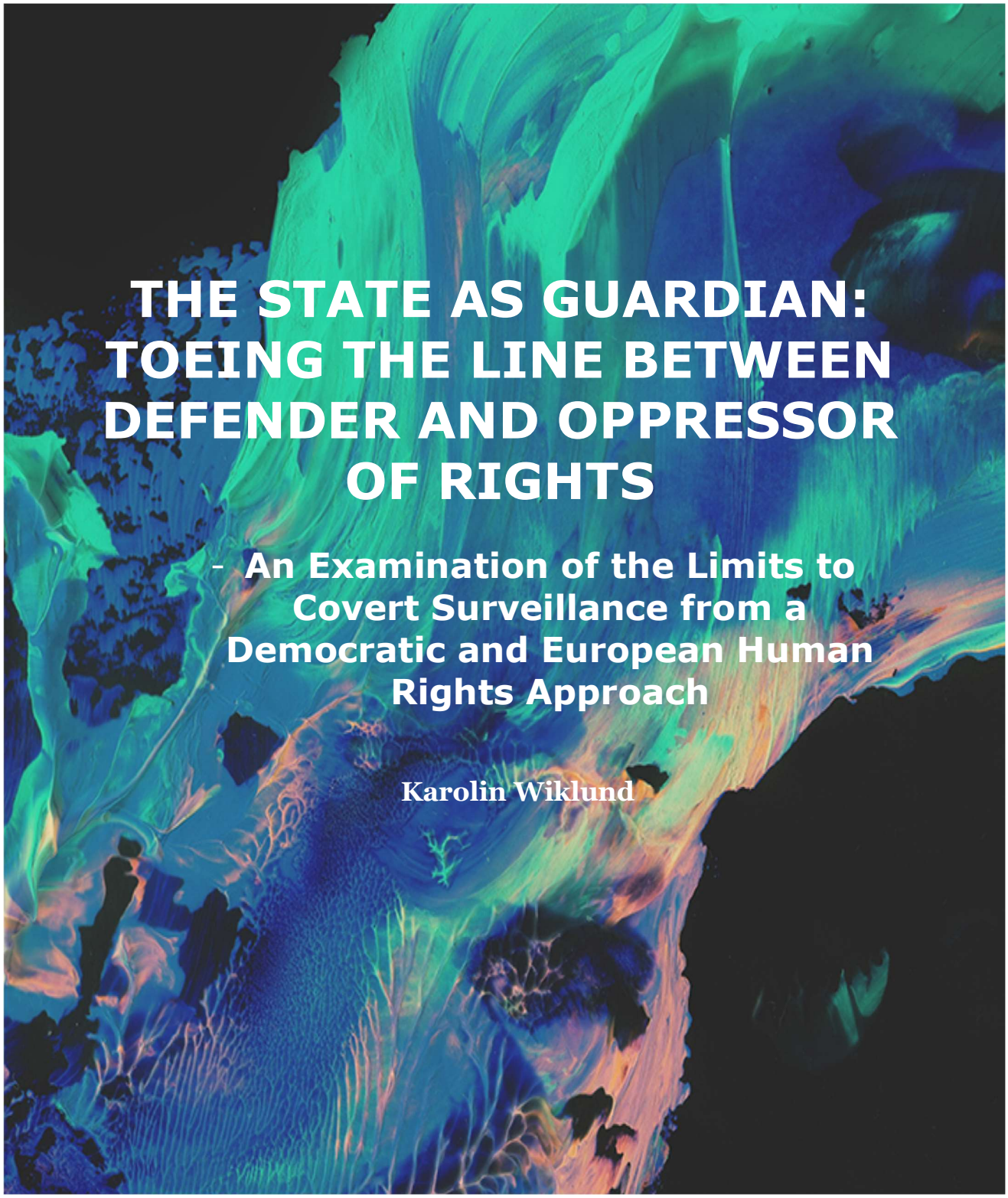
UMEÅ UNIVERSITY



THE STATE AS GUARDIAN: TOEING THE LINE BETWEEN DEFENDER AND OPPRESSOR OF RIGHTS

- An Examination of the Limits to Covert Surveillance from a Democratic and European Human Rights Approach

Karolin Wiklund

Fall semester 2022
Master thesis, 30 hp
Supervisor: Lena Landström

Abstract

In April 2022, the Swedish Government published the first interim report in a series of draft proposals on the introduction of new policiary surveillance measures in the wake of what seems to be one of the biggest surges of gang-related shootings and explosions in recent years. Like their counterparts, the draft proposal in SOU 2022:19 advocates for increased use of electronic surveillance measures to fight and prevent crimes committed in criminal environments. The Swedish Government is not alone in taking steps to improve public safety in a time characterised by political turmoil, violence, transnational crime and terrorism. Since 9/11, most European countries have turned towards domestic policies prioritising security over personal integrity and privacy. The privacy/security debate is, however, not only a matter of integrity. As many political rights depend on privacy, there is a worry that unchecked surveillance powers will be used to facilitate the growing trend of democratic backslide in Europe by spying on political dissidents, journalists and others questioning those in power. All of which leads to the question of how much surveillance democracy can withstand. By comparing the European human rights criteria for covert surveillance to the principles of just warfare, this essay tries to answer that question by analysing the legitimacy of covert surveillance from a rule of law and autonomy perspective in two steps. Firstly, by analysing the Swedish draft proposal in the light of the European Convention to understand the proposal's potential impact on privacy and secondly, by comparing which of the abovementioned regulations has the most democratic approach to privacy. The essay shows that while both frameworks contain democratic safeguards, just war theory contains more substantial protection, which makes the regulation more foreseeable and better equipped to confront the challenges of European securitisation. In building from this discussion, the essay concludes with suggestions on how to improve the consistency and effectiveness of privacy at a regional level.

Keywords: Securitisation; covert surveillance; privacy; public security; just war theory; European human rights.

Table of content

Abbreviations

BRÅ	The Swedish National Council for Crime Prevention
CJEU	The Court of Justice of the European
CJP	The Swedish Code of Judicial Procedure
CRF	The Charter of Fundamental Rights of the European Union
ECHR	The Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950
ECtHR	European Court of Human Rights
EU	The European Union
ICCPR	International Covenant on Civil and Political Rights of 16 December 1966
ICRC	The International Committee of the Red Cross
IHL	International Humanitarian Law
INCLO	The International Network of Civil Liberties Organizations
JWT	Just War Theory
LED	Directive (EU) 2016/680 on the protection of natural persons regarding processing of personal data connected with criminal offences or the execution of criminal penalties, and on the free movement of such data
SOU	Swedish Government Official Reports
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
UDHR	The Universal Declaration of Human Rights of 10 December 1948
UN	The United Nations
Venice	The European Commission for Democracy through Law Commission

1 Introduction

> The telescreen received and transmitted simultaneously. Any sound […] made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision […] he could be seen as well as heard […] How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. […] You had to live […] in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.[1]
>
> - George Orwell, 1984.

What differentiates democracies from autocracies? Most would probably say majority rule and the existence of free, fair and open elections. While those traits are inherently democratic, the recent democratic decline in countries such as Poland and Hungary show that universal suffrage and democratic processes are not enough to protect democracy.[2] By now, after several examples of autocratization worldwide, the pattern of democratic decline is familiar. A democracy is hit by a transformative election, and a new charismatic leader comes to power with promises to sweep away partisanship and bureaucracy. The leader rails against entrenched power structures and assures the people that the new government, unlike the previous one, is prepared to use extraordinary measures to cope with exceptional threats such as terrorism, economic crisis and political turmoil. Shortly after, new legal reforms are launched that remove checks on executive power, limit freedom of expression and abolish media pluralism in the name of public security. Add powerful surveillance technologies that enable the collection, communication and analysis of potential political adversaries, and we might as well be living in the Orwellian society of 1984.[3] Yet, advancing the common good often requires limitations on individual interests. Faced with terrorism, organized crime, and other risk generators, Europe has shifted towards increased surveillance and securitisation to respond to today's security challenges.[4]

While protecting the public is a legitimate goal and one of the primary functions of government,[5] the Snowden leak has opened the world's eyes to the danger of excessive surveillance, including the emergence of a culture of suspicion where collective action and expression of opinions are deterred out of fear and mistrust of the government.[6] In light of new evidence suggesting that several European Union (EU) countries have used illegal spyware to

[1] Orwell and Fromm, *1984*, 2–3.
[2] See Lührmann and Lindberg, 'A Third Wave of Autocratization Is Here', 1095, 1103.
[3] See Carothers and Press, *Understanding and Responding to Global Democratic Backsliding*, 10, 16; Scheppele, 'Autocratic Legalism', 545–46; Huq, 'Terrorism and Democratic Recession', 474; Roach, *The 9/11 Effect*, 14.
[4] See Lamer, 'From Sleepwalking into Surveillance Societies to Drifting into Permanent Securitisation', 393–94.
[5] See Taylor, 'To Find the Needle Do You Need the Whole Haystack?', 45.
[6] See Dencik, Hintz, and Cable, 'Towards Data Justice', 169, 176.

infect technical devices belonging to journalists, civil society organisations, politicians and lawyers,[7] the ability of human rights instruments and international courts to counter surveillance abuse has been questioned.[8] The European Court of Human Rights (ECtHR) has been accused of facilitating rather than hindering surveillance abuse by allowing domestic security narratives to stifle expectations as to what the rule of law requires.[9] Against this background, the question is whether human rights instruments such as the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and the Charter of Fundamental Rights of the European Union (CRF) are capable of safeguarding the right to privacy and the values of democratic societies. These issues are increasingly becoming topical in Sweden, which is experiencing one of the largest surges of violent crimes in modern times. In just one year, 61 people have died in presumed gang-related shootings, turning Sweden into the gun violence capital of Europe.[10]

Like many governments before them, the Swedish Government has turned to technology and the introduction of new security measures to solve the problem, which is evident in their recent proposals to increase state surveillance powers. Should the suggestions become a reality, the police would be allowed to use electronic surveillance in relation to a considerably larger group of people and types of crimes than before, even without concrete suspicion of criminal activity. But is it really proportional to subject innocents to surveillance on the off-chance that the information obtained might be used to solve a crime, and what about privacy? When did intrusions into people's private life without cause become anything other than unlawful? This essay explores these issues by addressing the European human rights requirements for covert surveillance in relation to the proposed changes to Swedish surveillance laws in SOU 2022:19, SOU 2022:50 and SOU 2022:52. How much flexibility do Convention States have in shaping their security policies, and how much flexibility should they be given? By highlighting the convergencies between the ECHR, national criminal law, and international humanitarian law (IHL), this essay delves into these issues by offering a new perspective on the democratic implications of increased state surveillance. It is believed that we are sleepwalking into a surveillance society, but is that really true, or is the threat to democracy exaggerated? In other words, how do we know when we have reached the democratic limit of covert surveillance?

[7] See Mazzini and Marzocchi, 'Pegasus and Surveillance Spyware'.
[8] E.g., Klamberg, 'Big Brother's Little, More Dangerous Brother'; Tsakyrakis, 'Proportionality', 484–87; Galetta and De Hert, 'Complementing the Surveillance Law Principles of the ECtHR with Its Environmental Law Principles', 73; Rojszczak, 'Surveillance, Legal Restraints and Dismantling Democracy', 5; Rusinova, 'A European Perspective on Privacy and Mass Surveillance at the Crossroads', 19–20.
[9] See Hirst, 'Mass Surveillance in the Age of Terror', sec. Conclusion.
[10] See BRÅ 2021:8, 10, 38; Polismyndigheten, 'Sprängningar och skjutningar'. The statistics refers to year 2022.

1.1 Aim and Objectives

Drawing on examples from the proposal by the Swedish Government to increase state surveillance powers,[11] this thesis aims to conceptualise and problematise the relationship between public security and privacy in European surveillance practices in light of core democratic principles. It further considers how the proposed changes to Swedish surveillance law would affect existing legislation and Sweden's commitment to European human rights instruments.

To achieve the overall aim of this thesis and to provide insight into the difficulties involved in balancing individual rights with the needs of the state, the following research questions will be used as guidance.

1. Under which circumstances and to what extent does the European human rights framework allow states to subject their citizens to covert surveillance in the interest of fighting crime? How does the Swedish legislative proposal fit within this framework?

2. How does 'civilian casualties'[12] treatment differ under just war tradition and the ECHR? What are the comparative advantages and disadvantages of the different approaches from a rule of law perspective?

3. Does the European human rights framework provide adequate privacy protection in relation to covert surveillance practices, or are enhanced safeguards necessary to respect the autonomy of individuals?

1.2 Previous Research Conducted on the Topic

Surveillance studies is an emerging multi-disciplinary field concerned with the broader implications of surveillance for individuals and society. It seeks to understand the rapidly increasing ways personal data are collected, stored, transmitted, checked and used to influence and manage people and populations – positively and negatively.[13] The research field connects to privacy studies, which is interested in how law can curtail surveillance and mitigate the risks

[11] The proposals can be found in SOU 2022:19, SOU 2022:50 and SOU 2022:52.
[12] In the context of this thesis, the term 'civilian casualties' refers to incidental harms inflicted upon non-liable individuals to achieve military or surveillance objectives, see Rønn och Lippert-Rasmussen, "Out of Proportion?", 12; Cohen och Zlotogorski, "Incidental Harm and the Analysis of Proportionality", 76–77 and chapter 6.
[13] See Lyon, 'Surveillance Studies', 1; Susser, 'Dialogue Data and the Good?', 298–99.

of data-driven technologies.[14] Since the terrorist attack in New York on September 11, much has been written about the conferral of new powers on national intelligence and law enforcement agencies for the purposes of counterterrorism and combating crime.[15] While the former has received quite a lot of public attention and academic critique,[16] the latter tends to attract less public and academic scrutiny, especially in a Swedish and Nordic context.[17] The closest thing to such a study is the dissertation by Ingvild Bruce, in which the preventive use of surveillance measures for the protection of national security in Dutch, Norwegian and Swedish law is compared through the lens of a democratic Rechsstaat.[18] Whereas Bruce's study focuses on "information gathering with the purpose of reducing the probability of harm to the territory, independence and sovereignty […] of a state"[19], this study is more interested in the justifications for surveillance to reduce the risk of crime and public harm.

Having said that, there are some Swedish studies that touch on similar subjects.[20] So far, most studies have focused on the legality and proportionality of Swedish surveillance measures from a predominantly constitutional point of view. In doing so, Björklund has focused on the value of public camera surveillance for crime prevention.[21] Others, such as Klamberg and Naartijärvi, have focused on the gradual expansion of electronic surveillance in Sweden, with particular attention to the legal mandates of the Swedish Security Service and the National Defence Radio Establishment.[22] In addition to these legal articles and essays, there is also an extensive legal

[14] See Susser, 'Dialogue Data and the Good?', 297–98.
[15] See Zedner and Ashworth, 'The Rise and Restraint of the Preventive State', 431.
[16] E.g., Daskal, 'Pre-Crime Restraints: The Explosion of Targeted, Noncustodial Prevention'; Molnar, 'Technology, Law, and the Formation of (Il)Liberal Democracy?'; Zedner and Ashworth, 'The Rise and Restraint of the Preventive State'; Lyon, 'Surveillance after September 11'; Goold and Lazarus, *Security and Human Rights*; Setty, 'Surveillance and the Inversion of Democratic Transparency'; Haggerty and Samatas, *Surveillance and Democracy*.
[17] As Ashworth, Zedner and Tomlin describes, "the use of […] criminal law and related coercive measures in a directly preventive way—have attracted little doctrinal or conceptual analysis (save in respect of counterterrorist measures)." See *Prevention and the Limits of the Criminal Law*, 1. This is especially true for the Nordic countries, see Piaseczny, 'The Determinants of Differing Legislative Responses in Similar States', 90.
[18] See Bruce, 'The Preventive Use of Surveillance Measures for the Protection of National Security - a Normative and Comparative Study of Dutch, Norwegian and Swedish Law'. Also see HusabØ,'Counterterrorism and the Expansion of Proactive Police Powers in the Nordic States'.
[19] Bruce, 'The Preventive Use of Surveillance Measures for the Protection of National Security - a Normative and Comparative Study of Dutch, Norwegian and Swedish Law', 20.
[20] E.g., Akdogan, 'Överskottsinformation från hemliga tvångsmedel –en analys av hur regleringen av överskottsinformation från hemliga tvångsmedel bör utformas, med särskilt beaktande av SOU 2018:61'; Hjertstedt and Landström, 'Domstolsprövning vid tvångsmedelsanvändning'; Landström, 'Hemliga tvångsmedel i brottsutredande syfte - Vem kan säga nej?'; Heuman, 'Vilka beviskrav gäller eller bör gälla för användningen av tvångsmedel?'; Beckman, 'Godtagbart i ett demokratiskt samhälle? De hemliga tvångsmedlen och rätten till personlig integritet. | SvJT'.
[21] See Björklund, 'Pure Flour in Your Bag'.
[22] Like Bruce, their studies mainly cover national security concerns. See Naarttijärvi, 'För din och andras säkerhet'; Klamberg, 'FRA and the European Convention on Human Rights'.

handbook written by Lindberg on the legal basis of pre-trial measures.[23] Despite raising important points about the ethics of government surveillance, none of the studies except Bruce's addresses the democratic implications of covert surveillance, or the role of international law in promoting democratic ideals, in particular detail. As such, this thesis hopes to contribute to the scholarly debate by raising awareness of the democratic issues associated with invoking public security as a rationale for expanding the scope, use and availability of covert surveillance measures in a crime-fighting context.

1.3 Method and Material

Critical discussion of balancing public security and privacy in covert surveillance practices requires different methodological approaches. To assess how useful a safeguard the European human rights framework is and could be in preventing abuse of surveillance powers, one needs to go beyond legal reasoning and what is traditionally understood as thinking as a lawyer. Thinking critically about the law is a two-stage process that starts with gaining knowledge and understanding of the law and ends with an evaluation of the legal issue at hand based on the argument's consistency with relevant norms, its persuasiveness and theoretical or ideological soundness.[24] When researching the permissible scope under European human rights law to restrict privacy for public security reasons, an analysis of current positive law (de lege de lata) is required.[25] The method most suitable for such an analysis is the legal-dogmatic research method which concerns researching current positive law as laid down in written or unwritten rules, principles, concepts, doctrines, case law and annotations in literature (in said order).[26]

The legal-dogmatic research method will also be used to describe Swedish surveillance law. When doing so, the main focus will be on the differences between current and proposed legislation, using preparatory works to clarify the legislation's intended purpose.[27] Although this study takes the context and law in Sweden as its primary focus, the goal of this thesis is not to provide an exhaustive overview of Swedish surveillance practices and how they relate to European human rights standards. The example only serves as a point of departure for a wider

[23] See Lindberg, *Straffprocessuella tvångsmedel : när och hur får de användas?*
[24] See James and Burton, 'Measuring the Critical Thinking Skills of Law Students Using a Whole-of-Curriculum Approach', 5–8.
[25] That is to say, how the law is. The term is often used in contrast to the term 'de lege ferenda' that refers to how the law should be. See Law, *A Dictionary of Law*, pt. de lege de lata, de lege ferenda.
[26] See Vranken, 'Exciting Times for Legal Scholarship', sec. 3.
[27] To the extent necessary, Swedish legal doctrine will also be used to understand the formation, development and understanding of privacy and surveillance laws in Sweden.

discussion of how the trend of securitisation in Europe affects democratic liberties. As such, this essay's legal analysis and conclusions will focus on the European - and not the Swedish - regulation of privacy.[28] Therefore, the arguments made in this essay apply equally to all European countries that employ similar surveillance practices as Sweden. The reason why Sweden was singled out as an object of comparison is threefold. Firstly, Sweden is a country whose constitutional privacy protection is heavily influenced by the ECHR.[29] Since the incorporation of the Convention in 1995, the ECHR has had the same legal status as ordinary law in Sweden, which means that all courts and administrative agencies are obliged not to apply norms in conflict with the Convention.[30] Secondly, Sweden has experienced a steep rise in both violent crime and counter-law[31] in recent years.[32] Lastly, Sweden is viewed as a 'full and stable democracy'[33] that takes great pains to avoid any practice that would hurt civic liberties.[34] Taking that and the inherent tensions between freedom and security into consideration,[35] Sweden makes an interesting object of study on the topic of compliance with human rights.

In terms of sources, the main weight of the research for the dogmatic parts of the paper is on a legal analysis of relevant case law from the ECtHR. In addition, legal commentaries have been used to understand how the Convention functions and how the right to privacy is generally understood in Europe.[36] Definitive answers as to how the right to privacy should be interpreted can, however, only be found in primary sources. In this case, the ECHR. The ECHR, like many other human rights instruments, does not specify the exact meaning of the rights ensured by the Convention. An interpretive authority is therefore needed to ensure that Convention rights are interpreted and applied in the same way, without national prejudices getting in the way.[37] The ECtHR, whose mission is to "ensure the observance of the engagements undertaken by the High

[28] For a more thorough overview of Swedish privacy and surveillance legislation, see Lindberg, *Straffprocessuella Tvångsmedel : När och hur får de användas?*
[29] Swedish constitutional law (2:6 Instrument of Government) was amended in 2009 to better comply with the integrity protection in the Convention. See prop.2009/10:80, 174–177.
[30] According to 2:19 of the Instrument of Government, "No act of law or other provision may be adopted which contravenes Sweden's undertakings under the European Convention for the Protection of Human Rights and Fundamental Freedoms". Also see prop.1993/94:117, 36–37.
[31] That is to say, the use of legal resources "to erode or eliminate traditional principles, standards and procedures of criminal justice." See Ericson, 'Security, Surveillance and Counter-Law', 6.
[32] See chapter 3.
[33] In the latest Democratic Index report from 2021, Sweden was ranked as one of the top four democracies in the world based on the country's electoral process and pluralism, functioning of government, political participation, political culture, and civil liberties. See Economist Intelligence, 'Democracy Index 2021', tbl. 12.
[34] See Shor et al., 'Does Counterterrorist Legislation Hurt Human Rights Practices?', 116.
[35] See Kennedy, 'The Structure of Blackstone's Commentaries', tit. The Fundamental Contradiction.
[36] E.g., Grabenwarter, *European Convention on Human Rights*; Schabas, *The European Convention on Human Rights*.
[37] See Killander, 'Interpreting Regional Human Rights Treaties', 145.

Contracting Parties" in "all matters concerning the interpretation and application of the Convention"[38], fulfils that role. In the case law concerning covert surveillance, the Court has focused chiefly on the right to privacy enshrined in Article 8 ECHR.[39] The right to privacy is also protected by EU law in Article 7 CRF, which is based on and corresponds to Article 8 ECHR.[40] From this perspective, going deeper into the EU regulation of privacy is redundant, should the interpretation of privacy by the Court of Justice of the European Union (CJEU) not deviate extensively, as the CJEU is obliged to interpret the meaning and scope of parallel rights in conformity with the ECtHR.[41] The ECtHR's case law concerning privacy therefore set the standard for all of Europe.[42]

When studying case law from the ECtHR, it is essential to remember that the Court works on a case-by-case basis. As explained by the Court, the ECHR is a living instrument that needs to be interpreted in light of present-day conditions.[43] Because of this, it is not certain that the Court would interpret a situation today in the same way as they did in the past, considering the different security needs of states and the rapid development of technology. Another methodological challenge concerning the Court's precedents[44] is the interrelation between domestic judicial mechanisms and the judgements of the Strasbourg Court. While the judgements of the ECtHR are binding on all Convention States, the Court relies on national courts for enforcement of Convention rights.[45] Since this study focuses on the substantive protection of privacy, the judicial enforcement of the right to privacy will be left out. Nevertheless, the case law of the ECtHR plays an integral part in shaping the human rights standard in Europe, which is evident by the deep impact of the Court's case law on European Government.[46]

[38] Article 19 ECHR; Article 32 ECHR.
[39] Under certain circumstances, articles 6, 9-11 and articles 13-14 ECHR might also be activated. See chapter 5.
[40] See Explanations relating to the Charter of Fundamental Rights (2007/C 303/02), 4.
[41] Article 53(3) CRF provides that in as so far both instruments contain corresponding rights, the meaning and scope of the rights laid down in the Charter shall be the same as those laid down by the Convention.
[42] All 27 EU Member States are parties to the Council of Europe and the ECHR, see Council of Europe, 'Map & Members'.
[43] E.g., *Tyrer v. the United Kingdom*, § 31; *Stec and Others v. the United Kingdom*, §§ 47–48; *Magyar Helsinki Bizottság v. Hungary*, §§ 120–122.
[44] Although the ECtHR does not operate on the basis of a system with biding precedents, the Court is known for constructing jurisprudence based on previous judgements. See Guillaume, 'The Use of Precedent by International Judges and Arbitrators', 13–14.
[45] Article 1 ECHR; Article 46 ECHR.
[46] See Keller and Stone Sweet, *A Europe of Rights*, 709.

Regarding the selection of relevant ECtHR case law, the choice of judgements for analysis was based on the content of the judgements. Besides limiting the selected case law to covert surveillance, the selection of cases was based on the judgement's relevance to public security in a crime-fighting context. As there is no clear organisational boundary between law enforcement and intelligence services across Europe, some of the selected cases deal with surveillance by intelligence services, despite their usual lack of participation in the prosecution of crime and the maintenance of public order.[47] The lack of clear definitional boundaries is also reflected in the Court's flexible definition of national and public security.[48] Because of this, many factors underlying the Court's assessment of covert surveillance in a national security context will also apply to matters of public security, making them relevant for this thesis's purposes as well.

While describing and understanding the rules of a legal system can be helpful when solving an issue within that legal system, such a dogmatic method is inadequate to answer questions about the usefulness of such a system, which is a central part of this essay (see research questions two and three). Therefore, the assessment of ECtHR case law on privacy is followed by a comparative analysis of the different approaches to privacy in JWT and democratic principles so that inconsistencies in the Court's case law can be brought to light and suggestions on improvements can be made.[49] The approach in international law to extract general principles from different jurisdictions is traditionally known as comparative law. In contrast to traditional comparative law, understood as the search for functional equivalents within other legal systems, this thesis takes on a broader perspective of comparative law that includes general jurisprudence of universal character that, while not always legally binding, has a decisive influence on the content of law.[50] As always, the challenge with comparative law is understanding the structure of principles developed in foreign legal systems.[51] The jurisprudence on privacy, for example, is more influenced by American scholars within the common law system than European scholars familiar with civil law.[52] Fortunately, most of the democratic principles used in this paper have such international spreading that understanding the core tenets should not be a

[47] See European Union Agency for Fundamental Rights., *Surveillance by Intelligence Services*, 28.
[48] See *Esbester v. the United Kingdom*, 9; Greer, *The Exceptions to Articles 8 to 11 of the European Convention on Human Rights*, 18.
[49] See page 51 and forwards.
[50] See Siems, *Comparative Law*, 149.
[51] See Eberle, 'The Method and Role of Comparative Law', 458, 478, 485.
[52] See generally, Szeghalmi, 'The Definition of the Right to Privacy in the United States of America and Europe Part III Developments in International Law'.

problem.[53] The same applies to the writings of legal philosophers such as Locke, Kant and Mill, whose liberal theories on freedom of conscience, autonomy and the private sphere have contributed to the formation of privacy and human rights as we know them today.[54]

Applying just war principles to define the legitimate scope of covert surveillance, on the other hand, is more controversial. The tradition of linking just war principles to surveillance practices originates from surveillance studies.[55] In just war theory (JWT), which is part of IHL, it is only permissible to subject civilians to harm if the strategic gain is significant enough compared to the harm inflicted.[56] Since the decision to subject individuals to covert surveillance includes similar considerations of just cause of action and proportional means, scholars such as Bellaby, Machnish, Rønn, and Lippert-Rasmussen suggest using just war principles when discussing just surveillance.[57] Given the recent critique of the ECtHR's capability of safeguarding privacy,[58] valuable insights could be gained by comparing how public security and privacy are balanced against each other in the jurisprudence of the Court and just war principles. In order to make a fair comparison between the frameworks, a rather extensive theoretical examination of them is needed. To compensate for the theoretically heavy parts of the paper, analytical elements and partial conclusions appear throughout the essay.

Owing to the fact that there is abundant of literature on the legitimate use of force and surveillance powers in democracies – both online and used in this paper – the selection of sources for the comparative analysis will be kept brief. Apart from the surveillance scholars mentioned in part 1.2 (mainly Solove, Regan, Gold and Lazarus), literature from others scholars active within the area has been used to understand the relationship between privacy and public security. For the sub-section of surveillance studies focused on JWT, the writings of the authors mentioned above have been most influential, given their expertise and authoritativeness in the area. Since the authors have already transferred the principles of just warfare into a surveillance context, the original writings on the use of force in IHL have only been examined briefly. The reliance on legal literature instead of primary sources of law is a consequence of this thesis's

[53] The rule of law and individual autonomy, for example, are important constitutional values in both the US and Europe. See Petkova, 'Privacy as Europe's First Amendment', sec. 2.3, 3.2.3. Also see part 4.3.
[54] See Freeden and Freeden, *Ideology*, 31; Biletzki, *Philosophy of Human Rights*, sec. 4 Liberal Underpinnings.
[55] See Robbins, 'Bulk Data Collection, National Security and Ethics', 170.
[56] See Ali, Rahim, and Bukhari, 'The Just War Theory and Human Rights Violations', 1–6.
[57] See Macnish, 'Just Surveillance?'; Rønn and Lippert-Rasmussen, 'Out of Proportion?'; Bellaby, 'What's the Harm?'. Other influential writings include Omand and Phythian, *Principled Spying*.
[58] See introduction.

aim to explore European surveillance practices *de lege ferenda*. To put it another way, one cannot put forward pragmatic, practice-driven solutions to legal issues without understanding why practitioners and scholars find them problematic and which legal solutions they prefer instead. Where democratic principles, such as respect for the rule of law, have had legal anchoring in European law, those sources have, of course, taken precedence as they have higher dignity. For a more comprehensive explanation of why JWT is the most appropriate starting point for designing an ethical framework for covert surveillance, see section 1.4 below.

1.4 Why Just War Theory?

The choice to use JWT as a comparative framework for the legitimacy of covert surveillance measures was based on many factors, some of which will be explained more in-depth in section 6.1 for contextual reasons. To start with, JWT is one of the oldest and most philosophically anchored frameworks on the use of legitimate state power,[59] which makes it a good starting point for assessing legitimate and illegitimate state action in the absence of equally well-established theories. The fact that JWT is as close to universally accepted as any international framework concerning national- or public security can reasonably be expected to be, is yet an advantage of JWT, as it makes it applicable in virtually any cultural and national context.[60] Thus, the use of JWT makes it methodologically easier to compare different standards of privacy, as JWT is less dependent on country-specific circumstances than other frameworks grappling with complex privacy and security issues, such as the Fourth Amendment Doctrine.[61] Based on the essay's purpose to conceptualise and problematise the relationship between public security and privacy in European surveillance practices, a broadly applicable framework was therefore best suited to avoid interpretative issues.

The framework is, however, not only suitable for legal comparisons for jurisdictional reasons. As will be discussed further in chapter 6, JWT is also an appropriate framework because of its content. Just like war can be a justified state response to armed attacks by non-state actors, covert surveillance can be a justified response to domestic threats of violence if done to prevent the occurrence of even greater harm. Since both intelligence collection and the use of armed force can be seen as sources of national power used by states to 'defend public interests and

[59] See M. Kinsella, 'Superfluous Injury and Unnecessary Suffering', 206.
[60] For the universal applicability of JWT, see Sassòli, *International Humanitarian Law*, chap. 4; chapter 6.
[61] The Fourth Amendment is the US equivalent to Article 8 ECHR, with the difference that the 4th amendment can only be used to challenge 'unlawful searches and seizes' and not other types of privacy intrusions. See Kohl, 'Data Protection Law Revealed', chap. 2.

manage peace and stability', the extension of JWT to covert surveillance is not as far-reached as one might think,[62] despite their differences in execution. To that end, JWT has been deemed the most appropriate ethical framework, besides Article 8 ECHR, to evaluate the moral and legal issues raised in this paper.

1.5 Structure

This thesis begins in chapter (1) with an introduction to the background of the study. The chapter outlines the aims and objectives of the thesis, gives a brief overview of previous research, presents key concepts, and discusses the research methods used in the study. After that, chapter (2) provides a background to the privacy and security debate in the context of surveillance. Chapter (3) then examines the surveillance measures currently debated in Sweden as a contextual backdrop to the securitisation trend. It considers the background and contents of the proposed changes to Swedish surveillance law and some public responses to the proposal. Following this, chapter (4) discusses the democratic implications of increased state surveillance with particular attention to its impacts on personal autonomy and the rule of law. The thesis then tries to identify the human rights requirements for covert surveillance in chapter (5) by looking at selected ECtHR case law. After giving an impression of the status quo and briefly commenting on the permissible scope to extend state surveillance powers in Sweden, chapter (6) looks at the treatment of civilian casualties under IHL and the ECHR to compare how the different frameworks approach the restriction of rights from a proportionality perspective. Drawing upon the conclusions made in the previous section, chapter (7) tries to answer whether the European human rights framework can address the challenges to privacy described in chapters 4 and 6. Finally, chapter (8) concludes by recapping salient points and suggesting directions in which surveillance policy can move to achieve a better balance between public security and privacy.

1.6 Terminology

Before going into the background of the privacy and security debate, some notes on terminology are in order to understand the conceptual framework on which this thesis relies on. *Surveillance* in a security context can be understood as "the targeted or systematic monitoring, by governmental organisations and their partners, of persons, places, items, infrastructures […] or

[62] See Gendron, 'Just War, Just Intelligence', 408.

flows of information, […] to enable, typically, a preventive, protective or reactive response."[63] Hence, *surveillance practices* are methods of information gathering. The surveillance practices relevant to this study are those that can be used for *covert investigation* of specific individuals in a criminal context. Typically, these include various forms of electronic surveillance such as telephone, email and video monitoring directed at subjects unaware of being part of a criminal investigation.[64] The study covers both traditional criminal investigations that start with reasonable suspicion of a crime and so-called proactive investigations that investigate the existence and behaviour of potentially dangerous persons and organisations to prevent serious crime.[65] Another term for this is *preventive policing,* defined as police action with the intention of identifying and intervening to stop a specific crime or a type of crime before or while it is carried out.[66] In Sweden, covert surveillance practices are referred to as *secret coercive measures* [hemliga tvångsmedel]. To ensure that Swedish legal terms are used consistently and correctly, the glossaries by the Swedish Parliament and the Swedish Courts will be used when translating Swedish terms into English.[67]

[63] Yaroyvi et al., 'SURVEILLE Deliverable 2.1: Survey of Surveillance Technologies, Including their specific Identification for further Work', 4.
[64] See Loftus and Goold, 'Covert Surveillance and the Invisibilities of Policing', 277, 282. In literature and case law, the term 'secret surveillance' is also used to describe covert actions, e.g. Cameron, *National Security and the European Convention on Human Rights*, 75. Also see *Klass and Others v. Germany*, §§ 42, 48; *Roman Zakharov v. Russia*, § 231;*Szábo and Vissy v. Hungary*, § 33. For this reason, the terms will be used synonymously in this essay.
[65] See Vervaele, 'Surveillance and Criminal Investigation', 123.
[66] See Sorell, 'Preventive Policing, Surveillance, and European Counter-Terrorism', 2.
[67] The dictionaries become especially relevant in chapter 3, which examines Swedish surveillance law. See Schweden, *Riksdagens flerspråkiga ordlista*; Courts of Sweden, *Svensk/Engelsk, Engelsk/Svensk Ordlista För Sveriges Domstolar = Swedish/English, English/Swedish Glossary for the Courts of Sweden*.

2 Setting the Scene – What is the Privacy vs Security debate about?

At its core, the privacy- and security debate is about protection. The protection of individuals from undue state coercion, or interference in their private lives, is a central part of the notion of privacy. In the same way as privacy includes an element of protection *from* the state, the notion of security includes an element of protection *by* the state. In its central role as guarantor of security, the state is obliged to protect citizens against threats to their well-being.[68] Therefore, surveillance technologies and laws are routinely defended and legitimized by narratives about what could happen and what must be prevented.[69] The state's duty to protect its citizens is a positive obligation in the sense that it is not enough for the state to react to acts of violence and aggression retrospectively by convicting and punishing those responsible.[70] States must also take active steps to ensure the 'security of a person'[71] by establishing legal safeguards against threats to life, physical integrity and arbitrary detention.[72] At the same time, states have a negative obligation to refrain from interfering with personal liberties, such as the right to privacy.[73] Since the state's duty encompasses both a positive obligation to secure the security of citizens and a negative obligation not to interfere with the private life of individuals, conflicts may therefore arise when the different interests collide.

2.1 Conceptualising privacy and security

Understanding the notion of privacy and security is not easy. In the words of Goold and Lazarus, "[i]n broaching the question of how to reconcile security with [privacy], we are in effect also asking how to balance between the individual and the collective, between the political and the legal, and between political sovereignty and the rule of law."[74] To determine what areas of one's personal ambit are legally protected, it is essential to clarify the term privacy and to distinguish between the concept of privacy and the *right* to privacy.[75] A proper understanding of the privacy

[68] See Weber and Staiger, 'Bridging the Gap between Individual Privacy and Public Security', 15, 18.
[69] See Lyon, Haggerty, and Ball, *Routledge Handbook of Surveillance Studies*, 106.
[70] See Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age', 118–19; Turner, 'A Positive, Communitarian Right to Security in the Age of Super-Terrorism', 50.
[71] As noted by Powell, there is no agreed legal definition ascribed to the 'right to security of a person' despite the concept being internationally recognized and sometimes treated as a human right on its own. See Powell, *Rights as Security*, 3, 10. Instead, the protection for individual security can be found in various human rights treaties such as the ECHR, the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).
[72] E.g., Article 2, 3, 5 ECHR; Article 6, 7, 9 ICCPR; Article, 3, 5, 9 UDHR.
[73] See Van der Sloot, 'Privacy as Personality Right', 26.
[74] Goold and Lazarus, *Security and Human Rights*, 7.
[75] See Rengel, *Privacy in the 21st Century*, 2.

and security debate also requires an examination of state responses to 9/11, given the impact of these events on the perception of acceptable security measures.[76]

2.1.1 The Meaning of Privacy

The recognition of privacy as an international human right can be traced back to the period following the Second World War.[77] The general discussion of privacy, however, is much older. References to privacy can be traced back to the inception of civilization and ancient texts such as the Babylonian Code of Hammurabi[78] (1750 BC), the Roman Codex of Justinianus[79] (533 AD) and the Quran[80] (610 AD). These ancient texts show that protection against unwanted intrusions into one's home has always been important. However, protecting the home is only one of the many aspects of privacy. Other aspects of privacy include privacy of one's person or body, privacy of behaviour and action, privacy of communications, privacy of data and image, privacy of thoughts and feelings and privacy of association.[81] As mentioned previously, the justifications for privacy as a value or interest is a separate issue from the question of how much protection privacy should be given as a right. The core of the legal right to privacy can be described as the prerogative of individuals to decide for themselves when, how, and to what extent information about themselves is communicated to others.[82] This is reflected in various human rights instruments, which describe privacy as the protection against 'arbitrary or unlawful interference with family, home or correspondence' as well as unlawful attacks against one's 'honour and reputation.'[83] While the need for privacy is closely related to the legal protection of privacy, not all values attributed to privacy, such as autonomy, democratic

[76] See Thimm, 'From Exception to Normalcy', 6.
[77] The recognition of the right emerged as a response to fascist regimes before and during the war. See Holvast, 'History of Privacy', 29.
[78] The Code of Hammurabi is one of the oldest complete set of laws, containing nearly 300 separate provisions of commercial, criminal, and civil law. See Lauren, 'The Foundations of Justice and Human Rights in Early Legal Texts and Thought', 164–65. Article 21 of the code states: "[i]f any one break a hole into a house (break in to steal), he shall be put to death before that hole and be buried." See 'The Avalon Project : Code of Hammurabi'.
[79] Under the code of the Emperor Justinian of Byzantium, a freeman could not be summoned from his home, as the code acknowledged the house as everyone's safest place, refuge and shelter. See Cuddihy, *The Fourth Amendment*, loc. Introduction.
[80] The Quran is the record of the revelations received by the prophet Muhammad during the period from 610 A.D. to 632 A.D. See Ringgren, 'Qur'an | Description, Meaning, History, & Facts | Britannica'. Al-Nur: 27 states: "O believers! Do not enter any house other than your own until you have asked for permission and greeted its occupants. This is best for you, so perhaps you will be mindful."
[81] Finn, Wright, and Friedewald, 'Seven Types of Privacy', sec. 3.
[82] See Westin, *Privacy and Freedom*, 7. A decrease in this 'ability' would be a loss of privacy.
[83] E.g., Article 17 ICCPR; Article 12 UDHR; Article 16 Convention on the Rights of the Child; Article 14 International Convention on the Protection of All Migrant Workers and Members of Their Families; Article 8 ECHR; Article 7 CRF; Article 11 American Convention on Human Rights. The explicit reference to reputation and honour is not included in all of the provisions.

deliberation and social-wellbeing, are legally protected or even labelled as privacy concerns.[84] As will be shown in chapter 4, these values nonetheless remain important for the discussion of the legitimate scope of covert surveillance.

2.1.2 Security as a politic rhetoric: 9/11 and the Human Rights Paradigm

Since 9/11, the political will worldwide has been more oriented towards the effective and efficient use of technology in the battle against crime and terrorism than protecting privacy, which is not surprising. During the last decades, the world has experienced a series of 'exogenous jolts' such as the London bombings, the Madrid train attacks and the Charlie Hebdo shootings, reminding us of the fragility of civic society and national infrastructure.[85] 'We must be willing to give up some privacy if it makes us more secure' is a common argument in favour of increased surveillance measures. Another one is that 'you shouldn't worry about government surveillance if you got nothing to hide.'[86] Those who favour the security first position argue that we will not be able to fight terrorism or function as a reasonably safe society if we do not modify some of our traditional constitutional norms limiting government powers.[87] For this reason, privacy is often construed as an obstacle to public security, which has a number of consequences. One example is the belief that privacy and security are mutually exclusive.[88] That claim is, however, not true. While security can weigh heavier than the interest of privacy, security never trumps privacy. Privacy, like all derogable rights, may be limited to the extent necessary to protect other vital interests after carefully examining the interests at stake.[89] Nevertheless, the perceived trade-off affects the political rhetoric of the privacy and security debate and makes it easier to override human rights concerns about introducing new, more far-reaching surveillance measures.[90]

[84] See Solove, 'Conceptualizing Privacy', 1093–94.
[85] Sedgwick, 'The Concept of Radicalization as a Source of Confusion', 480; Vasilopoulos, Marcus, and Foucault, 'Emotional Responses to the Charlie Hebdo Attacks', 1,15; Sajó and Uitz, *The Constitution of Freedom*, 440; Palmer, 'Dealing with the Exceptional', 520.
[86] See Solove, *Nothing to Hide*, 1.
[87] Westin, 'How the Public Sees the Security-versus-Liberty Debate', 119.
[88] See Moore, 'Why Privacy and Accountability Trump Security', 5.
[89] See Lustgarten and Leigh, *In from the Cold*, 9.
[90] See Smith, 'The Margin of Appreciation and Human Rights Protection in the'War on Terror': Have the Rules Changed before the European Court of Human Rights?', 141.

2.1.3 The Public Security Interest

Under what circumstances may privacy be limited, then? Most constitutions and human rights frameworks allow privacy restrictions on the grounds of national security or public safety.[91] Europe is no different. Under Article 8(2) ECHR, privacy may be restricted "[…] in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." Although protecting the general public is one of the primary duties of government, it is difficult to define public security as a singular concept.[92] One reason for this is the conceptual disarray concerning external and internal security (the protection of state sovereignty and the protection of social order). Since protecting the state often involves protecting the citizens and vice versa, public security tends to get confused with national security.[93] The fact that it is up to every country to decide what particular conduct is damaging to public security does not help with the conceptual disarray.[94] Still, it is important to distinguish between the two since the scope for introducing covert surveillance measures depends on the justification for the interference.[95]

Having said that, what is public security, and how is it different from national security? Put simply, public security refers to the physical and physiological safety of individuals from the aggression of others. 'Others' in this context may include persons of unsound minds, politically motivated terrorists and ordinary criminals.[96] National security is also concerned with protecting the state from external and internal threats, but from a different angle. While national security is generally directed at the well-being of the state, its territory and democratic institutions, public security is directed at the safety of individuals as a collective.[97] For this reason, sabotage, espionage and terrorism are often perceived as national security threats, while

[91] E.g., Article 4(2) ICCPR; Article 29(2) UDHR; Rengel, *Privacy in the 21st Century*, tit. Appendix: Privacy Protections in the Constitutions of Countries.
[92] See Friedman, 'What Is Public Safety?', 1.
[93] See Bislev, 'Globalization, State Transformation, and Public Security', 282; Manunta, 'What Is Security?', 59–61.
[94] According to Article 4(2) of the Treaty of the Functioning of the European Union (TFEU), matters of law and order and safeguarding national security remains the sole responsibility of each Member State. The ECtHR also considers public security as a prerogative of the Convention States. E.g., *M v. France*. "As far as the legal definition of criminal offences against […] public safety are concerned, the authorities of the particular State are best placed to decide whether a restriction designed to prevent such offences is necessary."
[95] The fact that a distinction is made between the two concepts in the first place, indicates that that human rights law treats national security matters differently from public security matters.
[96] See Bailey and Dammert, *Public Security and Police Reform in the Americas*, 11.
[97] See Bailey and Dammert, 1, 11; Aquilina, 'Public Security versus Privacy in Technology Law', 131–32. Also compare Article 29 with Article 33 of the Siracusa Principles.

targeted violence, organized crime and disregard for public order are perceived as public security threats.[98]

2.2 Currently Debated Security Trends

When looking at national surveillance laws in Europe, three trends catch the eye; (1) the shift towards pre-emptive justice in criminal law; (2) the normalisation of exceptional security measures; and (3) the expansion of the target population for covert surveillance.[99] In literature, this response to perceived threats to society is called securitisation[100] or the rise of the preventive state.[101] The intensification of covert surveillance measures is rooted in long-term national security policy shifts. What was initially part of a strategy to prevent terrorist attacks of the likes of 9/11 has evolved into a more general culture of control where surveillance is used to keep track of potential dangers to society.[102]

2.2.1 The Pre-emptive Turn in Criminal Justice

The pre-emptive turn in criminal justice has been described as one of the most notable features of the European security agenda in the past decade.[103] Compared to traditional criminal law, preventive or pre-emptive justice is more forward-looking and orientated towards stopping or preventing suspected acts of crime than investigating previously committed ones.[104] In this process, traditional principles, standards and procedures of criminal law, such as the presumption of innocence, are challenged.[105] In tracing the gradual erosion of these principles, Lacey describes how criminal law has regressed to include a range of character-based related evidence as a trigger for criminal investigation (as opposed to reasonable suspicion or serious

[98] See Bailey and Dammert, *Public Security and Police Reform in the Americas*, 12; Manunta, 'What Is Security?', 59.
[99] These trends will be explained in chapter 2.2.1–2.2.3. For a similar observation for trends in policing in general, see Van Brakel and Hert, 'Policing, Surveillance and Law in a Pre-Crime Society', 165.
[100] The term, coined by Buzan, Wæver and De Wilde in the 90s, refers to issues presented as existential threats requiring emergency measures and actions outside the normal bounds of political procedure. See Buzan, 'Rethinking Security after the Cold War', 13–14. Since then the term has been adopted by several scholars studying the impacts of surveillance on society, e.g. Cavelty and Leese, 'Politicising Security at the Boundaries', 52; Lamer, 'From Sleepwalking into Surveillance Societies to Drifting into Permanent Securitisation', 1.
[101] See Sajó and Uitz, *The Constitution of Freedom*, 440; Steiker, 'The Limits of the Preventive State', 774.
[102] See McGarrity, Lynch, and Williams, *Counter-Terrorism and Beyond*, 3–5.
[103] See Mitsilegas, 'The Preventive Turn in European Security Policy', 301; Lamer, 'From Sleepwalking into Surveillance Societies to Drifting into Permanent Securitisation', 393–94; Murphy, 'EU Counter-Terrorism & the Rule of Law in a Post-"War on Terror" World'; Crawford, *Crime Prevention Policies in Comparative Perspective*, xv.
[104] See Mitsilegas, 'The Preventive Turn in European Security Policy', 302; McCulloch and Wilson, *Pre-Crime*, 4.
[105] See Ericson, 'The State of Preemption: Managing Terrorism through Counter Law', 57.

indication of crime).[106] The assumption is that there is a finite number of 'bad people' with dangerous lifestyles and group affiliations, and if we can simply 'take out' enough of them, the world will be safer for those of good character.[107] Because of this, pre-emptive surveillance has been criticised for being discriminatory and reflecting a form of policing where due process, fairness and justice are not prioritised.[108]

2.2.2 The Normalisation of Exceptional Measures and Mission Creep

Several scholars have noted an expansion in both the arsenal of coercive policing methods employed by law enforcement agencies and the number of areas where their use is deemed appropriate.[109] The post-9/11 security rhetoric has not only had a significant impact on the normalisation of exceptional measures to combat terrorism but on other areas of criminal law as well. New police powers have often been introduced as counterterrorism measures but have then been made available to all or at least many other forms of criminal activities.[110] As Marrin puts it, "it is only a small leap to apply counterterrorism capabilities to track and catch individual lawbreakers and everyday criminals"[111] once a security rhetoric is already established. The asymmetry between clearly understood security benefits – in this case, crime reduction – and vaguely understood privacy harms (autonomy loss, self-censorship, discrimination etc.) is an incentive to continue using integrity-compromising practices with less severe types of crime.[112]

From a police point of view, the expansion of surveillance powers has significant advantages. Covert methods allow more flexibility in choices of tactics than ordinary police methods, require fewer resources and are said to increase the likelihood of multiple arrests. Furthermore, cover surveillance often removes the need for interview-based evidence.[113] If increased

[106] Compare Lacey, 'Explaining the Shifting Alignment of Ideas of Responsibility in the Vortex of Interests and Institutions: Towards a Political Economy of Responsibility in English Criminal Law', 156–57 to Vervaele, 'Surveillance and Criminal Investigation', 124.
[107] See Lacey, '5 Explaining the Shifting Alignment of Ideas of Responsibility in the Vortex of Interests and Institutions: Towards a Political Economy of Responsibility in English Criminal Law', 153–54.
[108] Van Brakel, 'The Rise of Preemptive Surveillance of Children in England', 7; Richards, 'THE DANGERS OF SURVEILLANCE', 2013, 1958; Ahmed, 'Citizenship, Belonging and Attachment in the "War on Terror"', 112.
[109] E.g., Flyghed, 'Normalising the Exceptional', 31; Hafetz, 'Military Detention in the "War on Terrorism"', 45–46; Monaghan and Walby, 'Making up "Terror Identities"', 146–47; Martins, 'Drones, Technology, and the Normalization of Exceptionalism in Contemporary International Security', 38–39.
[110] See Lachmayer and Witzleb, 'The Challenge to Privacy from Ever Increasing State Surveillance', 754.
[111] Marrin, 'Homeland Security Intelligence: Just the Beginning', 8–9.
[112] See Selinger and Rhee, 'Normalizing Surveillance', 60. In literature this is known as mission creep, see Lyon, Haggerty, and Ball, *Routledge Handbook of Surveillance Studies*, 236. Also see section 2.1.2.
[113] See Maguire, 'Policing by Risks and Targets', 319.

surveillance allows the police to combat crime more efficiently, why are scholars so anxious about this development? To begin with, there is the risk that states functioning as liberal democracies today might degenerate into defective democracies in the future. If so, there is a risk that surveillance infrastructure previously used for democratically legitimated purposes will be used to stifle free speech and persecute political dissidents.[114] Moreover, the application of 'traditional' anti-terrorism legislation to non-terrorist-related offences also raises questions about proportionality. Particularly whether disproportionately intrusive measures are taken against the perpetrators of minor crimes.[115]

2.2.3 Covert Surveillance of Non-Suspects

Another security trend is the shift from targeted to generalised surveillance.[116] In this context, generalised surveillance is defined as the imposition to disclose information on people not involved in criminal activity.[117] Suspicion is an essential characteristic of criminal law that determines when police action is justified and when it is not, i.e. when the limit for what constitutes an acceptable infringement of privacy has been crossed.[118] Despite this, there is a growing trend internationally to allow covert surveillance without reasonable suspicion.[119] Australia, for example, recently passed a law that enables comprehensive surveillance of criminal networks - and everyone loosely connected to those networks - through interception of communications by internet, text and other electronic means.[120] According to the Explanatory Memorandum of the law, it is enough that an individual is unknowingly engaged in or facilitating conduct that constitutes a relevant offence to be subjected to surveillance.[121] Similar laws have also been enacted in the US[122], the UK[123] and Canada.[124] Not even EU law

[114] Königs, 'Government Surveillance, Privacy, and Legitimacy', 13.
[115] See Maguire, 'Policing by Risks and Targets', 322, 326.
[116] Mitsilegas, 'The Preventive Turn in European Security Policy', 302.
[117] People who are engaged or suspected of being engaged in criminal activity are excluded from this definition. See Wallerstein, 'On the Legitimacy of Imposing Direct and Indirect Obligations to Disclose Information on Non-Suspects', 38.
[118] See Stoughton et al., 'Policing Suspicion', 38; Flyghed, 'Normalising the Exceptional', 28.
[119] Van Brakel and Hert, 'Policing, Surveillance and Law in a Pre-Crime Society', 169.
[120] Criminal Code Act 1995 (Cth), section 474.17; Division 6 of the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021.
[121] Explanatory Memorandum, § 318.
[122] In the US, Section 215 of The US Patriot Act and Section 702 of the Foreign Intelligence Service Act was used to authorize bulk collection of telephone and internet communications without individualized suspicion. Following the public outcry triggered by the Snowden revelations, the 2015 Freedom Act, which prohibits bulk collection of telecommunication metadata, was enacted. See Carpenter, 'Privacy and Proportionality', 36.
[123] Section 47(A) of the Terrorism Act 2000 allows the police to stop and search any person or vehicle within a specified area for a maximum period of 14 days, without reasonable grounds for suspicion.
[124] In 2010, a law was passed in Canada that empowered the police to arrest anyone near the G20 security zone who refused to identify themselves or agree to police searches. See Yang, 'G20 Law Gives Police Sweeping Powers to Arrest People'.

requires a link between data collection and individualized suspicion.[125] It only requires that law enforcement agencies distinguish between suspects and other parties relevant to the crime by limiting the processing of personal data of non-suspects to "specific conditions […] when absolutely necessary for a legitimate, well-defined and specific purpose." [126] Still, the question remains of how proportionate it is to subject all citizens to surveillance so that a few can be prevented from criminality.

[125] Article 6 Directive (EU) 2016/680 on the protection of natural persons regarding processing of personal data connected with criminal offences or the execution of criminal penalties, and on the free movement of such data.
[126] The latter is only an opinion expressed in the preparatory works. Article 29 Data Protection Working Party, 3.

3 Proposed Changes to Swedish Procedural Law

Situated in the post-9/11 war on terror rhetoric and the security trends mentioned above, the Swedish Government has progressively expanded the range of covert surveillance measures available to intelligence and law enforcement agencies to protect public safety.[127] The latest draft proposals concerning the expansion of secret coercive measures are just a few of many similar proposals in recent years, of which a vast majority have resulted in legislative changes.[128] What differentiates the latest proposals from the former ones is the clear divergence from the previously accepted view that the use of coercive measures without reasonable suspicion of criminal activity can only be justified under exceptional circumstances.[129] Because of this, the proposed changes to Swedish surveillance laws, which do not always require individualised suspicion for surveillance, have been described as a 'paradigm shift in Swedish criminal procedural law'[130] with potentially detrimental consequences to democracy.[131] At the same time, the Government has stressed the importance of more effective tools to combat gang-related crime considering the steep rise of violence and shootings with lethal outcomes in recent years, stating that "[t]he possibility of using secret coercive measures is absolutely central in the fight against these criminal environments."[132]

3.1 A Short Background to Swedish Surveillance Law

To better understand the recent developments in Swedish law, a brief background on Swedish surveillance legislation is necessary, starting with an overview of the applicable surveillance measures under current legislation. Before that, it should be mentioned that these coercive measures, like all coercive measures under Swedish law that can be seen as a "direct intervention against person or property in the exercise of public authority [own translation]",[133] constitute an exception to the constitutional rights and freedoms in the Instrument of Government.[134] When discussing the appropriate balance between privacy and public security, one should therefore keep in mind that constitutional protection is the main rule and police

[127] This pattern also applies to the other Nordic countries, see HusabØ, 'Counterterrorism and the Expansion of Proactive Police Powers in the Nordic States', 7–9.
[128] For an overview of these legislative changes, see chapter 5.1. in SOU 2022:19 and chapter 5 in SOU 2022:52.
[129] Compare SOU 1968:4,40; SOU 1975:95, 93; prop.1988/89:124, 43–44 to prop.2011/12:55,71–72; prop.2019/20:64, 124–125; SOU 2022:19, 271–273; SOU 2022:52, 155–159.
[130] See Sveriges Advokatsamfund, R-2022/1035, 3.
[131] See Civil Rights Defenders, 'Serious Criticism Against Proposal on Wiretapping Without Crime Suspicion'.
[132] Mikael Damberg quoted in Sveriges Radio, 'Government Open for Secret Police Surveillance and House Searches without Concrete Suspicion'.
[133] SOU 1995:47, 137.
[134] See chapter 2 Instrument of Government.

restraint the exception. However, before delving into such a discussion, it is essential to understand what types of surveillance measures exist in Swedish law and their effect on personal integrity.

3.1.1 Overview of Applicable Secret Coercive Measures

In Sweden, there are essentially five types of covert surveillance measures available to intelligence and law enforcement agencies, namely:

- *Secret interception of electronic communications* – the interception of messages sent to or from electronic communications networks in real-time or as recorded by technical means to read or produce the content of the message at a later time.[135]
- *Secret surveillance of electronic communications* – the acquisition of information through the same technical means as secret interception of communications, with the difference that the instrument can only be used to obtain information about the source and location of the data and not the content of the messages.[136]
- *Secret camera surveillance* – the optical surveillance of persons by remote and automatically operated cameras without the possibility of recording sound.[137]
- *Secret room surveillance or 'bugging'* – the monitoring and recording of conversations that none of the parties is aware of at meetings or other gatherings not available to the public.[138]
- *Secret data surveillance* – the use of special software to read and record messages on electronic devices such as computers, telephones and cloud services.[139]

Amongst these, the first four coercive measures have the longest history of application in Sweden – ranging from 1939[140] to 2008[141]. Secret data surveillance is a relatively new coercive

[135] See 27:18 CJP. It can be listening to oral communications such as telephone conversations or written messages in the form of text messages, images or e-mails, see SOU 2009:1, 60; prop.2011/12:55, 57–61.
[136] See 27:19 CJP; SOU 2022:19, 79.
[137] See 27:20a CJP; prop.1995/96:85, 38.
[138] See 27:20d CJP.
[139] See 1 § Secret Data Interception Act (2020:62). If permission is granted, law enforcement agencies may use spyware to activate cameras and microphones in the infected devices, see prop.2019/20:64, 105-109.
[140] The first law concerning secret coercive measures was adopted in 1939 and concerned the interception of telecommunications, see prop.1975/76:202, 24.
[141] As can be seen from the transitional provisions of the Act on Secret Room Surveillance (2007:978), secret room surveillance was introduced in January 2008.

measure that came into effect with the Secret Data Interception Act (2020:62) in April 2020.[142] Issues concerning covert surveillance are determined by the court upon the request of the prosecutor, provided that a delay would not endanger the investigation significantly. In such cases, covert surveillance may be authorized by the prosecutor in charge of the investigation while awaiting the court's decision.[143] Since the purpose of covert surveillance is to acquire information that the subject would not disclose voluntarily, the decision to undertake surveillance is made without notifying the subjects involved. Swedish law compensates this by the subject being notified of the surveillance after it has been terminated.[144]

3.1.2 The Separation Between Intelligence and Law Enforcement Agencies

The majority of the rules concerning secret coercive measures can be found in chapter 27 of the Swedish Code of Judicial Procedure (CJP). Given that Sweden has been relatively unscathed from right-wing extremism and terrorism compared to other countries, the shifting of the security/liberty border in Sweden has not been as decisive in Sweden as otherwhere. Consequently, most of the legislation concerning secret coercive measures has remained relatively unaffected by the move towards proactive policing and intervention at an earlier stage in the criminal investigation where a reasonable suspicion might not yet exist. The exceptions to this rule mainly concern terrorism and other spheres of criminal law with transnational dimensions.[145] In those cases, intelligence services may use covert surveillance outside criminal investigations to prevent severe crimes like terrorism, high treason and specific acts of violence and threats against representatives of public authorities.[146] Otherwise, the use of secret coercive measures in Sweden requires an ongoing policiary investigation where there is a reasonable suspicion of a committed crime of a certain penalty level or severity.[147] Separate rules therefore apply to intelligence and law enforcement agencies when it comes to the use of covert

[142] The Act is a temporary law which will remain in force for five years and terminate on 31 March 2025. The continued need for secret data surveillance will then be evaluated, see the transitional provisions of the Secret Data Interception Act (2020:62); prop.2019/20:64, 204.
[143] See 27:21 CJP; 27:21a CJP.
[144] See 27:31 CJP; prop.2002/03:74, 21. There are, however, some exceptions to the main rule, which mainly concerns information protected by rules of confidentiality. See SOU 2022:19, 90.
[145] See Lappi-Seppälä and Tonry, 'Crime, Criminal Justice, and Criminology in the Nordic Countries', 22–27; Beckman, 'Godtagbart i ett demokratiskt samhälle? De hemliga tvångsmedlen och rätten till personlig integritet. | SvJT', 1; Strandh and Eklund, 'Swedish Counterterrorism Policy', 363–64; Cameron, 'The Influence of 9/11 on Swedish Anti-Terrorism Policy and Measures', 209.
[146] The regulations can be found in the Act on Measures to Prevent Certain Particularly Serious Crimes (2007:979) and the Act on Collection of Data in Electronic Communication in the Crime Combating Authorities' Intelligence Service (2012:278).
[147] See part 3.2.1. An exception exists for secret surveillance of communications and secret camera surveillance. See 27:19, subparagraph 4 CJP; 27:20, second subparagraph respective 27:20c CJP.

surveillance in Sweden. Whereas the task of Swedish intelligence services is to 'prevent and detect offences against national security, fight terrorism and protect the central Government',[148] the task of the Swedish police is to 'prevent crime, monitor public order and safety and carry out criminal investigations.'[149] In view of this and the focus of this study on public security, the following sub-chapters will concentrate on secret coercive measures applied during criminal investigations by the police.

3.2 Timeline and Content of New Draft Proposals

In the autumn of 2020, the Swedish Government issued a terms of reference concerning the possibility of expanding the use of secret coercive measures in a crime-fighting context as a part of their 34-point program to combat gang violence.[150] The assignment of the Inquiry Chair was to take a position on whether secret coercive measures should be extended to crimes committed in criminal environments that are particularly difficult to investigate. More precisely, the Inquiry's task was to assess whether there is a need for new rules concerning secret coercive measures during preliminary investigations, especially regarding the need for new scales of penalties, extended crime catalogues and lowered suspicion requirements. The Inquiry Chair was also asked to consider how the protection of personal integrity would be affected by the legislative proposals and suggest strengthening measures if necessary.[151]

Later, in November 2021, the Government decided to expand the area of inquiry by launching a parallel investigation into the expansion of policiary covert surveillance outside the scope of preliminary investigations, as it is currently not allowed for the police to use covert surveillance preventively without prosecution being the main objective of the investigation.[152] The results of the inquiries were presented in SOU 2022:19, SOU 2022:50 and SOU 2022:52. All the reports concluded that increased covert surveillance was necessary and proportionate, considering the escalation of violent crimes in Sweden.[153]At the time of writing, the draft proposals have not yet resulted in legislative changes.[154] During the inquiry process, a new

[148] 3 § the Police Act (1984:387).
[149] 2 § the Police Act (1984:387).
[150] See Dir.2020:104, 1; Eriksson and Thornéus, 'Regeringens 34 punkter för att stoppa gängvåldet', sec. Regeringens "gängpaket" – 34 punkter mot gängvåldet.
[151] Dir.2020:104, 7–15; Dir.2022:13, 3.
[152] See Dir.2021:102, 1, 7, 13. Additional guidelines for the investigation can be found in, Dir.2021:113; Dir. 2022:32; Dir.2022:104.
[153] SOU 2022:52, 15–16; SOU 2022:50, 13; SOU 2022:19, 19–25.
[154] The majority of the legislative changes are proposed to enter into force in January 2024. See SOU 2022:19, 25; SOU 2022:50, 16; SOU 2022:52, 19.

Government also came to power in Sweden. The new Government is, however, of the same opinion as the previous Government regarding the best approach to combat gang violence and intends to legislate upon the proposals set forward, which will be described in the following sections.[155]

3.2.1 Extended Crime Catalogues

Today, covert surveillance during preliminary investigations is limited to offences in respect of which a less severe penalty than imprisonment for two years or more is not prescribed and a list of enumerated crimes related to national- and public security, like war instigating and endangering of the public.[156] Coercive measures also require that the requested information is particularly important [*av synnerlig vikt*] to the criminal investigation.[157] The government wants to expand the categories of offences that can give rise to covert surveillance to less severe crimes, such as extortion, perjury and sexual offences directed towards children with only pecuniary penalties.[158] They also want to introduce a new 'penalty valve' [*straffvärdesventil*] that allows for secret coercive measures in cases where an individual is suspected of having committed multiple offences which, taken individually, are not severe enough to justify surveillance.[159] The expansion of the number of crimes that can give rise to covert surveillance does not only apply to traditional pre-trial investigations. In the draft proposal concerning preventive surveillance measures (SOU 2022:52), it is suggested that law enforcement agencies should be able to use secret surveillance of electronic communications, secret interception of electronic communications, secret camera surveillance and secret data surveillance (with the exception of sound recording devices) to prevent certain crimes carried out within groups or organisations.[160] The media portrays the proposed legislative changes as exceptional measures

[155] See Sverigedemokraterna et al., 'Tidöavtalet: Överenskommelse För Sverige', 19; Government of Sweden, 'Statement of Goverment Policy', 5.
[156] The same applies if the circumstances at hand are such that it can be assumed that the offence will result in a minimum of two years of imprisonment or more. See 27:18, second subparagraph CJP; 27:19, second subparagraph CJP; 27:20a, second subparagraph CJP; 27:20d, second subparagraph CJP; 27:23a CJP; 4 § Secret Data Interception Act (2020:62).
[157] 27:20 CJP; 27:20b CJP; 27:20e CJP. According to the preparatory works, this means that the measure must have a positive effect on the investigation that is both tangible and significant. While the information obtained does not necessarily have to lead a conviction, it has to contribute to the continuation of the investigation more than just insignificantly. In principle, this means that the investigation should not be able to be carried out by other means. See Ds Ju 1981:22, 88; prop.1988/89:124, 44–45; SOU 2022:19, 83.
[158] The complete list of suggested offences includes gross unauthorized data access, sexual offences towards children, aggravated hunting offences, serious insider trading and, with the exception of minor offences, extortion, perjury and interference in a judicial matter. See SOU 2022:19, 178. Amongst the offences directed towards children grooming can be found, which is an offence with a fine in the penalty scale (6:10 a Swedish Penal Code).
[159] See SOU 2022:19, chapter 6.14.
[160] See SOU 2022:52, 185–186, 208.

to combat particularly serious crimes. According to the Minister of Justice, the measures seek to target the most threatening crimes to society.

> It is about ensuring that the police and prosecutors have access to the same tools as the Swedish Security Service when it comes to, for example, crimes of terror or espionage, but in well-defined cases – it will target the most serious crimes and criminals moving in gang environments [own translation].[161]

When reading the actual draft proposals, it is evident that the proposed measures are more far-reaching and do not always connect to typical gang-related or systematic crime, at least not when it comes to pre-trial measures. Extortion, for example, does not only take place in criminal networks. According to the Swedish National Council for Crime Prevention (BRÅ), extortion is just as common, if not more common, when it comes to violence in close relations, divorce proceedings, disputes among young people and business disagreements.[162] The discrepancy is not as significant in the area of preventive coercive measures. Still, it represents a substantial change from the current legislative framework, which is limited to crimes that typically fall within the jurisdiction of the Security Service.[163] Should the new proposal become a reality, the police would not only be granted *preventive* surveillance powers of this capacity for the first time, but they would also be able to use covert surveillance in relation to less system-threatening crimes than before, including murder, kidnapping, grave narcotics- and weapon crimes.[164]

3.2.2 Derogations from the Suspicion Threshold

The perhaps most recognized and criticized proposal of them all is the proposal to allow covert surveillance without factual reasons to believe that a specific person is involved in criminal activity, both for pre-trial[165] and preventive criminal investigations.[166] If the national parliament accepts the proposal to lower the requirement of suspicion for pre-trial investigative measures, secret interception of communications and secret data surveillance would no longer require that someone is reasonably suspected [*skäligen misstänkt*] of a crime.[167] That is to say, that it is more probable than not that the suspect has committed the crime under investigation.[168]

---

[161] Gunnar Strömmer, quoted in an interview with TT, 'Hemliga tvångsmedel ska stoppa gängvåld'.
[162] See BRÅ 2012:6, 10–13, 33–44, 54; BRÅ 2012:12, 53–54, 103–104.
[163] See part 3.1.2; 1 § Act on Measures to Prevent Certain Particularly Serious Crimes (2007:979).
[164] For the complete crime catalogue, see SOU 2022:52, 217.
[165] Several of the consultative bodies have expressed concerns about the proposal. See, e.g., Institutet för mänskliga rättigheter, Dnr 1.1.2–283/2022, 3; Uppsala Universitet, JURFAK 2022/26, 2; The Swedish Commission on Security and Integrity Protection, Dnr 87–2022, 5.
[166] See Separate statement of opinion of Sargon de Basso in SOU 2022:52, 344.
[167] See SOU 2022:19, 289.
[168] Lindberg, *Straffprocessuella Tvångsmedel: När och hur får de användas?*, 89; Ekelöf et al., *Rättegång. 3*, 44.

3.2.2.1 Formulation of Suspicion for Pre-trial Investigative Measures

In short, the proposed changes would lower the threshold for using covert surveillance (in real-time and in the past) by prescribing a more lenient requirement of suspicion, where an investigative need to find out who *might* reasonably be suspected of a crime in the future is enough for surveillance. According to the Inquiry Chair and the Swedish Prosecution Agency, the amendments are necessary to make progress in criminal investigations related to criminal networks, as those responsible often hide behind layers of digital infrastructure.

> This applies, for example, in cases where there are indications that a person is hiding behind a particular telephone number, electronic address or communications equipment […] Another example is cases of murder, where there is reason to believe that the injured party and the offender were in contact with each other prior to the murder [own translation].[169]

The proposal would target (a) those who might be suspected of having committed a crime; (b) persons suspected of possibly having taken part in a crime; (c) and individuals who might be contacted by those specified in a and b if there are particular reasons to believe that attempts of contact will be made.[170] Essentially, this would open up for a regulation where everyone in close proximity to either the place of a crime or a person connected to a crime could be subjected to surveillance. That is to say, the friends, family and work colleagues of suspects or possible suspects.

3.2.2.2 Preventive Surveillance and the Open Police

In the same way as the increased risk to the lives and health of innocent bystanders to gang violence has been a decisive factor in the decision to lower the suspicion requirement for surveillance measures applied during preliminary investigations, the increased risk to innocents has been central to the inquiry concerning the introduction of preventive surveillance measures for law enforcement agencies.[171] As noted before, the biggest difference between preventative and reactive surveillance is the connection between action and criminality.[172] When the Act on Measures to Prevent Certain Particularly Serious Crimes was introduced in 2007 and gave intelligence services the opportunity to use covert surveillance as a preventative measure to

[169] SOU 2022:19, 22. Also see the Statement of Opinion of the Swedish Prosecution Authority, ÅM2022-1189, 4–5.
[170] The surveillance is limited to telephone numbers, electronic address, communication equipment and readable information systems. The authorisation is dependent on the information being of particular importance to the investigation. See chapter 9.10 in SOU 2022:19.
[171] Compare SOU 2022:19, 263–272 to SOU 2022:52, 155–159.
[172] See part 1.3, 1.5, 2.2.2 and 3.1.1.

detect and deter certain system-threatening crimes, it was discussed whether the open police should have the same opportunities to use preventive surveillance. Although preventive surveillance was presented as an effective tool in the fight against serious crime, the Inquiry considered it inappropriate to extend police surveillance more than had already been done since preventing future crimes is not part of the mission of the police.[173] The introduction of policiary preventive surveillance therefore stopped at particularly serious crimes adjacent to or at least as serious as the crimes under the jurisdiction of the Security Service.[174]

Another aspect of the reluctance to expand preventive police surveillance powers beyond the most society-threatening crimes has to do with proportionality. It was argued that the 'identified need' for such measures was insufficiently substantiated in relation to its usefulness and that the police should focus more on social policy measures to prevent crime instead.[175] Now, after reconsidering the issue in light of today's security concerns, it is the opinion of both the Government and the new Inquiry Chair that there is a need for policiary covert surveillance measures that can be applied without a concrete suspicion of criminal activity.[176] The extended scope is proposed to apply in relation to the crime catalogue described in part 3.2.1.[177] Although the proposal is not limited to criminal networks, the bill's primary purpose is to address the social problems caused by gang violence. To ensure that the regulatory framework can deter serious criminal activity, regardless of the context in which it is committed, the Inquiry suggests that the authorisation should apply to persons within groups or organisations at significant risk of engaging in criminal activity.[178]

3.2.3 Personalised Instead of Location-Based Surveillance

Alongside the suggestions above, the Government suggests that authorisation for secret camera surveillance, secret room surveillance and secret data surveillance thereof should be linked to the suspect in addition to specific locations,[179] such as vehicles, parks, residential buildings or shopping centres.[180] Under current legislation, those kinds of measures are only allowed in

[173] See Ds 2005:21, 158–161; prop.2005/06:177, 44–49.
[174] See 1 § the Act on Measures to Prevent Certain Particularly Serious Crimes (2007:979); prop.2005/2006:177, 40–42.
[175] This view is reflected in, inter alia, SOU 2012:44, 230, 476–478, 533–535, which is a review of the Act on Measures to Prevent Certain Particularly Serious Crimes (2007:976). For similar considerations also see, SOU 1998:46, 389–390; prop.2005/06:177, 43.
[176] See chapters 7.4.2, 8.2.4 and 8.4.2 in SOU 2022:52.
[177] See SOU 2022:52, 217.
[178] See SOU 2022:52, 207–208.
[179] See SOU 2022:19, 327.
[180] SOU 2022:19, 314.

places where there is a reason to believe that the suspect or person under investigation will be present.[181] The limitation has to do with the principles of purpose, need and proportionality in Swedish law. Following these principles, coercive measures may only be used for the purposes stated in the legislation if there is an obvious need for it and the intended purpose cannot be achieved with other less intrusive means. The measure must also be reasonably proportional to the benefits resulting from and the intrusion or harm entailed by the action.[182] To make such an assessment and ensure that the privacy of suspects and innocent bystanders is not violated without cause, the deciding authority (in this case, the court) must know which places might be subjected to surveillance.[183] Be that as it may, crime-fighting authorities find it hard to predict the whereabouts of suspects since criminals "are very much aware of the possibility of being subjected to surveillance […]" and try to meet at places "where they feel safe to speak [own translation]."[184] Because of this, the Swedish Prosecution Authority wants to tie surveillance permits to suspects instead of locations so that the use of coercive measures is better adapted to the needs of law enforcement, which is a sentiment echoed by the Government.[185] For the time being, the proposal only applies to surveillance measures used during preliminary investigations. However, in view of the statement of the Inquiry Chair in SOU 2022:19 that there may be a need to review the provisions in other contexts as well, the issue is currently also being examined in relation to preventive surveillance measures.[186]

3.3 Summary and Thoughts About the Proposal

In conclusion, the proposed changes to Swedish surveillance law give law enforcement agencies a wider scope of discretion[187] and open up the possibility of proactive policing by the open police.[188] The lowering of the suspicion threshold for surveillance and the expansion of the types of offences that may give rise to surveillance fit into the general trend of securitisation worldwide. From a Swedish point of view, however, the suggestions represent a clear divergence from how matters of security and privacy have previously been handled, indicating

[181] 27:20b CJP; 27:20e CJP; 3 § the Act on Measures to Prevent Certain Particularly Serious Crimes (2007:976).
[182] The principles can be derived from 2:12 of the Instrument of Government and chapter 24–27 CJP. See prop.1995/96:85, 29.
[183] Prop.2013/14:237, 97; prop.2019/20:145, 14.
[184] SOU 2022:19, 306.
[185] Chapter 10.4 SOU 2022:19.
[186] See SOU 2022:19, 306; Dir. 2022:104, 3–4.
[187] This is because a lower standard of criminal suspicion makes it easier for prosecutors and law enforcement agencies to request authorisation for covert surveillance by the court as less evidence of criminal wrongdoing is necessary.
[188] That is to say, the part of the Swedish law enforcement that deal with preliminary investigations and not national intelligence. See chapter 3.1.2.

a shift in attitude regarding the ‘appropriate’ use of surveillance measures. As the level of domestic turmoil has increased in Sweden, the willingness of the legislator to allow more intrusive surveillance measures seems to have grown with it. The attitude shift is especially noticeable in the field of preventive surveillance, where the legislator, up until this point, has been reluctant to give the police more preventive powers. A likely explanation for the shift could be that the threat to life and health has become more imminent than before, when acts of violence were less frequent and did not have the same connection to organised crime and terrorism.

4 Effects of Surveillance on Core Democratic Values

The traditional structure of democracy includes people with the right to live largely private lives and a government whose workings are transparent to its constituents because it is empowered by the people to act in their name.[189] Yet, commonplace surveillance practices share a set of non-democratic characteristics. They each open up to examination and control of citizens while constraining individual autonomy. They are conducted against people with little knowledge of the inner workings of the systems or their rights as citizens. As with most technological systems, they also resist public participation by means of their opaque design.[190] Therefore, covert surveillance practices may undermine democratic governance and citizens' fundamental rights if not subject to sufficient safeguards.[191] Because of this, privacy is often said to be a necessary component of democracy, as it is impossible to exercise political rights, such as freedom of expression, without the free and undisturbed development of one's personality.[192] Hence, to know whether surveillance practices accord with the requirements for democratic governance, it must be determined to what extent these practices serve the aim of core democratic principles.

4.1 The Key Characteristics of Democracy

Although there are several models and perceptions of democratic government, the modern concept of democracy tends to involve two major characteristics. The first is the existence of the rule of law rather than the existence of arbitrary exercise of state powers, and the second is public participation.[193] Public participation involves having a say in decisions that affect one's life. This means citizens must be informed about and have the opportunity to provide input about the activities and decisions of their representatives.[194] The EU adhere to this definition of democracy and considers "respect of human rights and fundamental freedoms […] respect for the rule of law […] access for all to an independent justice system [*and*] a government that governs transparently and is accountable to the relevant institutions and to the electorate"[195] as intrinsic parts of *democratic governance.* This is recalled by Article 2 and Article 6 of the consolidated Treaty on European Union (TEU) and the Preambles to the Treaty and the CRF.

[189] Setty, 'Surveillance and the Inversion of Democratic Transparency', 28.
[190] See Monahan, 'Surveillance as Governance', 91.
[191] See Born and Caparini, *Democratic Control of Intelligence Services*, 3.
[192] E.g., Goold, 'How Much Surveillance Is Too Much? Some Thoughts on Surveillance, Democracy, and the Political Value of Privacy', 42–43.
[193] See Campos and André, *Challenges to Democratic Participation*, pt. Introduction.
[194] See Johnson and Wayland, *Surveillance and Transparency as Sociotechnical Systems of Accountability*, 21.
[195] COM (2006) 421 final, 5.

4.2 Personal Autonomy

Having defined what is meant by 'democratic governance', the following sections will move on to discuss the principles that together form the backbone of modern democracy, starting with autonomy. Autonomy is one of the core concepts of legal and political thought. Having autonomy means being able to be self-governing or self-determining.[196] Privacy protects the individual interest in autonomy because it creates a space around individuals where they can direct their lives as they see fit, irrespective of social and political pressures.[197] It enables individuals to experiment and come up with new, controversial or deviant ideas – which is essential for societal development and progress.[198] Because of this, privacy protection also encompasses protection for the right to self-development and autonomy in Europe.[199]

4.2.1 Theoretical Underpinnings – from Kant, Mill to Habermas and Beyond

The legal, philosophical discussion of autonomy originates from the Enlightenment and thoughts on the proper boundaries of the state. Inspired by philosophers such as Locke, the idea of society as a social contract emerged, and the private domain received non-negotiable status.[200] The social contract is based on the notion that the state has arisen out of a simultaneous agreement among free individuals to give up some of their freedom in exchange for basic security and shelter.[201] The justifications for individual restraint depend on showing that everyone, in some way, would consent to them since it is every man's right to execute 'the law of nature.'[202] Since then, legal philosophers such as Kant, Mill, Habermas and Meiklejohn have continued to promote different notions of autonomy as a restraint on government power.[203] The Millian concept of autonomy rests on the view that interference with one's private life should only be allowed when individuals cause harm to someone.[204] What constitutes 'harm' according to Mill is not clear from his writings. Given Mill's liberal background and absolute defence of

[196] See Dworkin, *The Theory and Practice of Autonomy*, 1, 6.
[197] See Mokrosinska, 'Privacy and Autonomy', 118.
[198] See Boehme-Neßler, 'Privacy', 228; Richards, 'THE DANGERS OF SURVEILLANCE', 1948.
[199] See e.g., *Pretty v. United Kingdom*, § 61; *Christine Goodwin v. the United Kingdom*, § 90; *El-Masri v. the former Yugoslav Republic of Macedonia*, § 248; *A.H. and Others v. Russia*, § 383. Also see Article 2 TEU; Judgement of 21 December 2016, *Post-och telestyrelsen, and Secretary of State for the Home Department v Tom Watson, Peter Brice and Geoffrey Lewis*, joined cases C-203/15 and C-698/15, EU:C:2016:970, §§ 92–93.
[200] See Lincoln, *The SAGE Handbook of Qualitative Research*, 140–41, 145.
[201] As Locke writes, people enter into the social contract to obtain "a secure enjoyment of their properties, and a greater security against any that are not of it". See Locke and Cox, *Second Treatise of Government*, 110.
[202] See Locke and Cox, 135.
[203] These arguments for autonomy can be found in; Meiklejohn, 'The First Amendment Is an Absolute'; Mill et al., *On Liberty*; Kant, *Practical Philosophy*; Habermas, *The Structural Transformation of the Public Sphere*.
[204] See Mill et al., *On Liberty*, 80.

"free moral and intellectual development"[205], mere dislike and distress caused by certain behaviours are not enough for state intervention. Accordingly, for an act to be harmful, some perceptible damage like death, physical injury or financial loss is required.[206] Meiklejohn and Habermas agree with Mill on the importance of allowing individuals to develop on their own.[207] In Habermas's view, democracy depends on the possibility of public deliberation, which requires specific forms of communication between citizens, secured in what he calls the 'public sphere.'[208]

4.2.2 Privacy as a Gateway for the Enjoyment of Political Rights

As autonomy is more of a philosophical than a legal concept, privacy advocates have had a hard time explaining to the public why they should care about their privacy or the privacy of others. This stems from a long tradition of viewing privacy as an individualistic value, focused on maintaining relations with others and promoting individual flourishing. When viewed as a collective right affecting more than just one individual, understanding the societal benefits of privacy is easier.[209] As Regan notes:

> Aligning privacy with societal interests […] remove some of the difficult philosophical and policy issues involved in reconciling the balance between individual and society […] and may result in stronger policies supporting privacy.[210]

Privacy, for example, is embedded into the voting process in secret ballots as it allows citizens to communicate preferences without fearing that their actions will be ridiculed or susceptible to intimidation.[211] In addition to this, privacy facilitates freedom of expression and association. The awareness or belief that a group or an idea is a target for surveillance might contribute to a hesitance to interact with that surveilled group or ideas for fear of falling under surveillance themselves, creating an atmosphere of fear, distrust and avoidance of engaging in public or collaborative activities.[212] As history has shown and is still true today, the state has misused

[205] Mill et al., 152.
[206] See Riley's interpretation of Mill in , *Mill on Liberty*, 98.
[207] As Meiklejohn writes, "we, the people who govern, must try to understand the issues which, incident by incident, face the nation", which is only possible if voters are self-government. See Meiklejohn, 'The First Amendment Is an Absolute', 255.
[208] See Habermas, *The Structural Transformation of the Public Sphere*, sec. V; Habermas, Habermas, and Habermas, *Reason and the Rationalization of Society*, 17.
[209] See Regan, *Legislating Privacy*, 1995, 28; Goold, 'How Much Surveillance Is Too Much? Some Thoughts on Surveillance, Democracy, and the Political Value of Privacy', 44.
[210] Regan, *Legislating Privacy*, 1995, 231.
[211] See Adler and Hall, 'Ballots, Transparency, and Democracy', 151.
[212] See Raab, 'Surveillance', 270.

covert surveillance to keep track of people with religious or political views that are considered extreme or contrary to the state.[213] Thus, excessive restraints on privacy can create a chilling effect on essential liberties to democracy.

4.3 The Rule of Law as Theory and Practice

The rule of law can be described as the modern-day equivalent of the social contract. As Galetta and De Hert explain, the rule of law defines the proper balance of power between the state and its citizens. It is a system for imposing legal accountability of citizens who have wronged the state (or the collective) and a means to empower citizens whom the state has wronged.[214] In other words, the rule of law is concerned with the restraint of arbitrary power. Under the rule of law doctrine, no one – not even the highest official – is above the law.[215] There is no moment in which the whim of a given actor may justifiably cancel or suspend the laws that govern their actions. Most importantly, all rules derive authority from the people through their elected representatives.[216]

4.3.1 Essential Components of the Rule of Law and Rule of Law as a European Value

As previously mentioned, the EU is built on respect for the rule of law, which is one of the founding values of the Union and the backbone of modern democracy.[217] At its core, the rule of law requires that government officials and citizens are bound by and act consistently with the law.[218] Different legal jurisdictions have different understandings of what the rule of law entails. In literature, there is a distinction between 'thick' maximalist and 'thin' minimalist rule of law. Both notions include a set of procedural aspects: regulations must be laid down in advance, be clear and certain in their content, be accessible and predictable for the subject, and be applied equally to everyone. If those conditions are met, the legal system is said to be valid.

---

[213] Various human rights organisations and news entities report that covert surveillance has been used to spy on Muslim communities without cause; to jail human rights defenders, lawyers and journalists; to intercept the communications of politicians, activists, priests, businesspeople and other public figures. E.g., Pilkington, 'NYPD Settles Lawsuit after Illegally Spying on Muslims'; INCLO, 'Surveillance and Democracy: Chilling Tales from Around the World', 7–8; International Service for Human Rights, 'China's Abuse of National Security to Curtail Human Rights'; Amnesty International, 'Georgia Archives'; Ball, 'NSA Monitored Calls of 35 World Leaders after US Official Handed over Contacts'.

[214] See Galetta and de Hert, 'Effects of Surveillance on the Rule of Law, Due Process and the Presumption of Innocence', 238.

[215] See Dicey, *Introduction to the Study of the Law of the Constitution*, 114.

[216] The opposite of the rule of law is authoritarian rule, which places all public power at the hands of one ruler whose decisions are unconstrained by law and lack public deliberation. See O'Donnell, 'Why the Rule of Law Matters', 34, 35, 38.

[217] COM/2014/0158 final, 2.

[218] See Tamanaha, 'A Concise Guide to the Rule of Law', 2.

The 'thick' version also incorporates a set of substantive ideals of justice, fairness and respect for fundamental rights, which are said to be based on or derived from the values which underpin the rule of law.[219] Maximalist approaches to the rule of law are followed by the United Nations (UN), the EU and the European Commission for Democracy through Law (the Venice Commission[220]), which considers governance in accordance with the values of democracy as core elements of the rule of law.[221] More specifically, respect for the rule of law from a European perspective requires:

> that the principles of legality implying a transparent, accountable democratic and pluralistic law-making process; legal certainty; prohibition of arbitrariness of the executive powers; effective judicial protection, including access to justice, by independent and impartial courts; and separation of powers, be respected.[222]

4.3.2 Challenges to The Rule of Law from Covert Surveillance

From a 'thick' maximalist rule of law perspective, the ability of covert surveillance practices to sort people into different categories might be a challenge to the rule of law as judgements on an individual's moral worth and right to belong in society made "on the basis of whether his or her body and behaviour 'fit', rather than on the basis of whether they have committed any kind of offence"[223] raises questions about fair treatment and equality. In surveillance literature, the "ways in which large-scale practices of observation and monitoring facilitate profiling and screening of social groups"[224] is called social sorting.[225] Although some kind of risk categorisation is necessary for the police to allocate their resources where best needed, concerns have been expressed about the potential of covert surveillance to re-enforce existing prejudices

[219] See Burnay, *Chinese Perspectives on the International Rule of Law*, sec. 1.6; Versteeg and Ginsburg, 'Measuring the Rule of Law', 104; Møller and Skaaning, 'Systematizing Thin and Thick Conceptions of the Rule of Law', tbl. 1.
[220] The Venice Commission is the advisory body of the Council of Europe on constitutional matters. The Commission provides non-binding legal advice to its member states. See Resolution Res. (2002) 3, *Adopting the Revised Statute of the European Commission for democracy through Law*, CDL (2002) 27.
[221] UN Security Council, *The rule of law and transitional justice in conflict and post-conflict societies : report of the Secretary-General*, S/2004/616, 23 August 2004, para 6; European Commission for Democracy through Law (Venice Commission), *Report on the Rule of Law - Adopted by the Venice Commission at its 86th plenary session (Venice, 25-26 March 2011)*, Study No. 512/ 2009, CDL-AD (2011) 003 rev., Strasbourg, 4 April 2011, para 37; Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council of 16 December 2020 on a general regime of conditionality for the protection of the Union budget, para 3.
[222] Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council of 16 December 2020 on a general regime of conditionality for the protection of the Union budget, para 3.
[223] Morgan and Pritchard, 'Security and Social "Sorting"', 126.
[224] See Arroyo Moliner and M. Frowd, 'Social Sorting'.
[225] The term social sorting is attributed to David Lyon and his work, *Surveillance as Social Sorting*. See Monahan, 'Editorial: Surveillance and Inequality', 219.

and racial biases,[226] which is not entirely unfounded. Research on investigatory stops shows that black individuals are not only more likely to be stopped by the police for reasons unrelated to criminal behaviour,[227] but that they are also more likely to be subjected to physical force during such interactions.[228] Similarly, Canadian studies show that people who belong to Muslim communities or have Arab names experience more trouble with false positives on no-fly lists than other Canadian citizens.[229] Although there is no official figure on how many people might have been delayed or prevented from travelling because of a false positive on a no-fly list, it is estimated that up to 100 000 Canadians could be affected, Muslim or not.[230]

4.4 Some Thoughts on Surveillance and Democratic Principles

Taking into account what has been said in the previous sections, covert surveillance needs to be regulated in a statute that is accessible to the people and allows them to understand under what circumstances they might be subjected to surveillance for it to be in accordance with the rule of law. Moreover, it needs to secure the private life of citizens against arbitrary exercise of police powers by placing obstacles in the way of disproportionate or discriminatory application of surveillance laws. As noted on several occasions, public security is such a powerful aspiration that it tends to trump all other considerations, which is problematic considering the value of privacy for key democratic principles. Therefore, it is unfortunate that the privacy-security debate is often framed in individualistic terms, as the long-term effects of the loss of privacy for society extend beyond the impacts on those personally affected. Against this background, the following chapters will examine to what extent existing human rights standards can protect against aggressive pre-emptive surveillance practices that can result in chilling effects and the gradual drift to tyranny without proper limitations on state power.

[226] See Lyon, *Surveillance as Social Sorting*, 20–21.
[227] The statistics are derived from American and British research. See e.g., Yesufu, 'Discriminatory Use of Police Stop-and-Search Powers in London, UK'; Kramer and Remster, 'Stop, Frisk, and Assault?'; Bowling and Phillips, 'Disproportionate and Discriminatory'.
[228] See Kramer and Remster, 'Stop, Frisk, and Assault?'
[229] See Nagra and Maurutto, 'No-Fly Lists, National Security and Race'.
[230] See No Fly List Kids, '100k Canadians – #NoFlyListKids'; Fife, 'Up to 100,000 Canadians Could Be Affected by No-Fly List, Research Suggests - The Globe and Mail'.

5 Human Rights Requirements for Covert Surveillance

As already discussed, the ECHR provides the most elaborate and detailed human rights framework for discussing European covert surveillance measures. The Convention, as interpreted by the Court, stipulates the minimum standard of European privacy protection. Therefore, the Court's jurisprudence functions as a 'normative template' for surveillance practices during criminal investigations.[231] The gathering of evidence during criminal proceedings and the prevention of crime through covert surveillance raises several issues under the Convention, the right to privacy under Article 8 ECHR being only one of them. The more procedural aspects of covert surveillance can be found in Article 6 and Article 13 ECHR, which guarantee the right to a fair trial and the right to an effective remedy.[232] Depending on the context, covert surveillance might also interfere with an individual's expressive, political and religious rights under Articles 9-11 ECHR.[233] Should the beforementioned rights be violated in a discriminatory way, Article 14 of the Convention might also be engaged.[234]

5.1 The Scope of the Right to Privacy and the Occurrence of an Interference: Some General Remarks

Although covert surveillance may infringe upon a number of Convention rights, the primary article engaged in relation to surveillance practices is still Article 8 ECHR.[235] The right to respect for private and family life is structured in two parts: the first paragraph defines the scope of the right, and the second paragraph sets out the permissible restrictions. First, the Court examines whether the issue at hand falls within the scope of one of the protected interests of the article. That is to say, a person's private life, family life, home or correspondence. Then, after it has been established that the issue covers at least one of the four interests, the Court examines whether there has been an interference by looking at the criteria for permissible

[231] Chapter 1.3.
[232] E.g., *Bykov v. Russia*, § 69–83, in which the usage of evidence obtained through unlawful secret surveillance rendered a trial unfair under Article 6. Insufficient safeguards in relation to judicial oversight and notification after the termination of covert surveillance measures might also engage Article 13. See *İrfan Güzel v. Turkey*, § 96.
[233] In the case of *Big Brother Watch and Others v. the United Kingdom,* §§ 442–458, the ECtHR found that the bulk interception regime in the UK violated the right of journalists to protect their sources under Article 10 as well as their right to privacy under Article 8. Likewise, the disclosure of information about personal religious convictions might engage both Articles 8 and 9. See *Folgerø and Others v. Norway*, § 98. Should authorities use geolocation data to physically locate those wishing to assembly, Article 11 ECHR might also become relevant. See Bernal, 'Data Gathering, Surveillance and Human Rights', 256.
[234] For example, if secret surveillance is used for racial, sexual or political profiling.
[235] See Bernal, 'Data Gathering, Surveillance and Human Rights', 252.

restrictions set out in paragraph 2.[236] Justified interferences include the prevention of disorder or crime and the protection of public safety. The protection of public security is therefore a legitimate aim under Article 8(1) ECHR. For the interference to be permissible under Article 8(2), it must be "in accordance with the law and […] necessary in a democratic society." In its jurisprudence, the ECtHR has given shape to this clause by developing a 'democratic necessity test' consisting of a review of the interference's legality, necessity and proportionality.[237]

5.1.1 Protected Interests and Interferences in Relation to Covert Surveillance

In the same way, as the concept of privacy encompasses a large number of interests incapable of exhaustive definition,[238] the scope of protected interests under Article 8 ECHR is difficult to define categorically.[239] The use of covert technology devices for crime-fighting purposes has been found to fall within the scope of multiple Article 8(1) interests, starting with *Klass v. Germany,* where the secret monitoring of telephone conversations was recognized as an interference with the applicant's private life and correspondence. Other communications covered by the notion of private life include communication over the internet and email.[240] Since the police entering a house without the resident's consent already constitutes a violation of the privacy of one's home, there is reason to believe that secret monitoring in the home is also covered by the notion.[241] Which legally protected interests are at stake is, however, not an important question for the Court. Since the essential object of Article 8 is "to protect against arbitrary interferences […] by a public authority"[242], all kinds of investigative measures mentioned in chapter 3 fall under the scope of Article 8(1).[243]

In the context of covert surveillance, the question of whether there has been interference is also a non-issue. The very existence of secret surveillance measures or legislation permitting such practices interferes with the right to privacy. With regard to the highly intrusive nature of surveillance measures and the fact that many of the subjects are oblivious to the interference, it is enough for the applicant to show that he or she is a potential target of surveillance to be

[236] See Schabas, *The European Convention on Human Rights*, 366–67; Grabenwarter, *European Convention on Human Rights*, 204–6.
[237] E.g., Greer, *The Exceptions to Articles 8 to 11 of the European Convention on Human Rights*, 9, 14–15; Gerards, 'How to Improve the Necessity Test of the European Court of Human Rights', 467–68.
[238] For a discussion of the concept of privacy, see chapters 2 and 4.
[239] See Kilkelly, *The Right to Respect for Private and Family Life*, 10.
[240] *Kennedy v. the United Kingdom*, § 118; *Bărbulescu v. Romania*, § 131.
[241] See Grabenwarter, *European Convention on Human Rights*, 202.
[242] *Libert v. France*, § 43.
[243] As reiterated by the Court in *Zoltán Varga v. Slovakia,* § 2, in principle all "measures of secret surveillance and storage, processing and use of personal data […] fall within the scope of the notion of private life."

considered a victim. This is to ensure that the secrecy of surveillance practices does not result in the measures being effectively unchallengeable and outside the supervision of national judicial authorities and the ECtHR.[244]

5.1.2 Legality, Necessity and Proportionality of Surveillance Measures

When justifying interferences under Articles 8-11 ECHR, the ECtHR uses the 'necessary in a democratic society test', consisting of three steps.[245] The first step concerns *legality*. The interference must have a basis in national law, be accessible to the individuals concerned, have foreseeable consequences and be compatible with the rule of law.[246] In a surveillance context, this takes on a special meaning. As repeated by the Court on several occasions, there is a greater risk for abuse in situations with extreme urgency, where states must act quickly to counter serious threats to society based on information prevented from disclosure because of secrecy.[247] For this reason, the Court argues that the significance of judicial safeguards cannot be overestimated, given the "widespread practice of transferring and sharing […] intelligence retrieved by virtue of secret surveillance" in state practices and the large amount of "information retrievable by the authorities applying" such measures.[248] Against this background, the ECtHR has developed six minimum safeguards, commonly referred to as the Huvig/Weber criteria, that should be set out in law to avoid abuses of power.[249] These are:

> (1) the nature of offences which may give rise to an interception order; (2) a definition of the categories of people liable to have their communications intercepted; (3) a limit on the duration of interception; (4) the procedure to be followed for examining, using and storing the data obtained; (5) the precautions to be taken when communicating the data to other parties; and (6) the circumstances in which intercepted data may or must be erased or destroyed.[250]

[244] *Klass and Others v. Germany*, § 34; *Kennedy v. the United Kingdom*, § 124; *Roman Zakharov v. Russia*, §§169–172; *Szabó and Vissy v. Hungary*, §§34–39; *Ekimdzhiev and Others v. Bulgaria*, §§ 291–292.
[245] See Greer, *The Exceptions to Articles 8 to 11 of the European Convention on Human Rights*, 7.
[246] *Weber and Saravia v. Germany*, § 84.
[247] E.g., *Malone v. the United Kingdom*, § 81; *Centrum för rättvisa v. Sweden*, § 49.
[248] *Szabó and Vissy v. Hungary*, §§ 78–79.
[249] *Huvig v. France*, § 30; *Valenzuela Contreras v. Spain*, § 59; *Weber and Saravia v Germany*, § 95; *Roman Zakharov v. Russia*, 231; *Szabó and Vissy v. Hungary*, § 55; *Ekimdzhiev and Others v. Bulgaria*, §§ 291–293. For bulk surveillance there are additional criteria which requires that the law sets out the precautions taken when communicating material to other parties and which procedures there are for authorisation and ex post review of covert surveillance measures. See *Big Brother Watch and Others v. the United Kingdom*, §§ 361–364; *Centrum för rättvisa v. Sweden*, § 275.
[250] *Centrum för rättvisa v. Sweden*, § 249.

The second and third step involves *necessity* and *proportionality*. Interferences must be supported by relevant and sufficient reasons and be proportionate to the legitimate aims pursued.[251] When the Court reviews the proportionality of a surveillance measure, they often ask themselves the four following questions: (i) does the measure adopted pursue a legitimate aim? (legitimacy); (ii) can it serve to further that aim, at least to a certain degree? (suitability); (iii) is it the least restrictive measure to achieve that aim? (necessity); and (iv) all, in all, do the ends justify the means? (strict proportionality).[252]

5.1.3 The Margin of Appreciation in Security Matters

Due to the proximity of national authorities to sensitive and complex issues being determined at a national level, a certain level of discretion is given to the Convention States in determining the presence of a pressing social need and the nature and scope of derogations necessary to avert it.[253] This holds true, especially for matters of public- and national security. In the Court's view, "it falls in the first place to each Contracting State, with its responsibility for 'the life of [its] nation', to determine whether that life is threatened by a 'public emergency.'"[254] A standpoint later reaffirmed in *Klass v. Germany* and *Leander v. Sweden* in an intelligence and crime-fighting context, considering the increased gravity of contemporary security threats (including the scourge of global terrorism, human trafficking and cyberattacks).[255] Despite leaving the assessment of what policy might be the best in the fields of national security and the prevention of disorder and crime to the domestic authorities, Convention States may not adopt whatever measures they deem appropriate in view of the risk that covert surveillance might undermine democracy.[256]

In weighing the balance of interests in surveillance cases, the Court looks at the legitimate aim pursued by the state in relation to the level of intrusion imposed upon the individual. For covert surveillance to be justified, the Court must be satisfied that there are adequate and effective safeguards against abuse which depends on an overall assessment of the nature, scope and duration of surveillance measures, as well as the grounds required for ordering them. Where a

[251] *Segerstedt-Wiberg and Others v. Sweden*, § 88.
[252] See Bachmaier Winter, 'Proportionality, Mass Surveillance and Criminal Investigation: The Strasbourg Court Facing Big Brother', 326.
[253] See *Handyside v. the United Kingdom*, § 48.
[254] *Ireland v. the United Kingdom*, § 207.
[255] *Klass and Others v. Germany*, §§ 49–50; *Leander v. Sweden*, §§ 59–60. Also see *Big Brother Watch and Others v. the United Kingdom*, §§ 322–323, for an overview of security challenges facing European states today.
[256] See *Klass and Others v. Germany*, §§ 49–50; *Bărbulescu v. Romania*, § 112; *Segerstedt-Wiberg and Others v. Sweden*, § 88; *Centrum för rättvisa v. Sweden*, § 113.

particularly important facet of an individual's identity is at stake, the margin tends to be narrower. The margin also tends to be more limited where the right at stake is crucial to the individuals' enjoyment of key rights or when there is no consensus on the subject within the Convention States.[257]

5.2 The Strasbourg Court on the Scope of Criminal Intelligence

Although the Huvig/Weber criteria mentioned in part 5.1.2 are recognized as the standing benchmark for compliance with Article 8 ECHR in cases of targeted surveillance, the principles give surprisingly little guidance in terms of adequate and inadequate privacy protection. To be able to reach a conclusion about the permissible scope of covert surveillance measures in a definite sense, a closer reading of the Court's case law focusing on the reasoning behind introducing the principles in the first place is therefore required. The same applies to the principles of legality, necessity and proportionality since the Huvig/Weber criteria is an extension of the three general criteria for assessing restrictions on Convention rights.

5.2.1 Nature of Offences and Activities Giving Rise to Surveillance

The placement of microphones, cameras and electronic spyware in private places is considered among the most privacy-invasive measures available to the police since they disclose very intimate details about a person's conduct, opinions and feelings.[258] For this reason, the Court believes that only crimes of a certain gravity should be able to give rise to covert surveillance during criminal investigations.[259] In the words of the Court, "such monitoring may be used only if there are grounds to suspect that a serious offence is being planned or is or has been committed, and only if the establishment of the facts by other methods are deemed unlikely to succeed."[260] While there is no definition of 'serious crime', ECtHR case law suggests this may include: organised crime[261], bomb attacks against state officials and state targets,[262] drug

[257] See *Uzun v. Germany*, § 63; *Roman Zakharov v. Russia*, § 232; *Gaughran v. the United Kingdom*, § 77.
[258] See *Kruslin v. France*, § 33; *Vetter v. France*, § 26; *Uzun v. Germany*, §§ 51, 66; *Khadija Ismayilova v. Azerbaijan*, § 116; *Ekimdzhiev and Others v. Bulgaria*, § 394.
[259] In the CJEU's case law on privacy, the limitation of covert surveillance to serious offences is even more apparent. In accordance with the principle of proportionality, only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying interference with Articles 7 CRF. See Judgement of 21 December 2016, *Post-och telestyrelsen, and Secretary of State for the Home Department v Tom Watson, Peter Brice and Geoffrey Lewis,* joined cases C-203/15 and C-698/15, EU:C:2016:970, § 102; Judgement of 2 March 2021, *H.K. v. Prokuratuur*, C-746/18, EU:C:2021:152, § 33.
[260] *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, § 79.
[261] *Malone v. the United Kingdom*, § 81.
[262] In *Uzun v. Germany*, § 80, the ECtHR considered that surveillance via GPS was proportionate to the legitimate aims pursued and thus necessary in a democratic society, as the surveillance concerned "several attempted murders of politicians and civil servants by bomb attacks."

trafficking, aggravated assault and other crimes compromising the physical well-being of others, such as armed robbery.[263] Examples of crimes and legislation on the nature of offences which may give rise to surveillance not meeting this threshold include minor theft[264], drunk driving[265], and legislation allowing "secret interception of communications in respect of a very wide range of criminal offences."[266] In between petty stealing and extreme dangers to society, such as terrorism[267], there is a rather extensive grey area of crimes unaddressed by the ECtHR. The recent development in the Court's case law also seems to indicate that the ECtHR is letting up the severity requirement expressed in *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* when it comes to crime prevention.[268] In *PN v. Germany*, for example, the Court found that the retention of photographs and cellular samples of a repeat offender of handling stolen goods was proportionate even though the applicant had not been found guilty of a particularly serious offence.[269] Another example is *Adomaitis v. Lithuania*, in which the Court found suspicion of corruption-related activity serious enough to engage surveillance powers even though the crime had no impact on the physical well-being of the country's citizens.[270]

5.2.2 Categories of Persons That Can Be Placed Under Covert Surveillance

The categories of people that can be placed under surveillance depend on the surveillance context. Surveillance by the police in criminal investigations almost always requires suspicion directed towards the surveillance target, which has to do with necessity and proportionality.[271] Prior suspicion of criminal activity safeguards against arbitrary and disproportionate interferences with privacy, which is also why lawyers, political activists, journalists, and other people performing democratic functions enjoy greater privacy protection than other categories

[263] *Peruzzo and Martens v. Germany*, §§ 6–15, 46–50. The case concerned the collection and storing of cellular material in a DNA- database for the purposes of facilitating the investigation of possible future crimes. Also see *P.G and J.H v. the United Kingdom*, § 49, for the Court's stance on armed robbery.
[264] See *M.K. v. France*, §§ 41, 46-47.
[265] See *Gaughran v. the United Kingdom*, §§ 97–98.
[266] *Roman Zakharov v. Russia*, § 244. For similar reasoning see, *Iordachi and Others*, §§ 43–44.
[267] *Kennedy v. the United Kingdom*, § 190.
[268] See footnote 260.
[269] *P.N v. Germany*, §§ 80–91. Even though the case does not concern covert surveillance it should be able to give some guidance on the Court's view of proportionality given how "closely related" these issues are. See *S. and Marper v. the United Kingdom*, § 99. Also see *M.K v. France*, § 30; *P.N v. Germany*, §§ 61–63, for more references between data retention and covert surveillance.
[270] The protected interest in this case was the protection of transparency and openness of public service. See *Adomaitis v. Lithuania*, § 84.
[271] See *Weber and Saravia v. Germany*, § 125; *Iordachi and Others v. Moldova*, § 51; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, § 79; *Roman Zakharov v. Russia*, § 260; *Szabó and Vissy v. Hungary*, § 71; *Dragojević v. Croatia*, § 94; *Karabeyoğlu v. Turkey*, § 103; *Adomaitis v. Lithuania*, § 81; *Mustafa Sezgin Tanrıkulu v. Turkey*, §§56–57.

of people.[272] For a short period of time, the existence of 'factual indications for suspecting the involvement of a person in the planning, execution or commitment of a criminal act' also encompassed intelligence services.[273] That is to say, the part of national authorities tasked with detecting threats to national security based on communications belonging to a large number of individuals that are later filtrated and analysed according to selected risk factors.[274] Following the landmark judgements of *Big Brother Watch and Others v. the United Kingdom* and *Centrum mot rättvisa v. Sweden*, this no longer holds true. After considering the differences between the activities of national security intelligence services and criminal investigative authorities, the ECtHR found it unreasonable to hold bulk surveillance to the same threshold of suspicion as targeted criminal surveillance, given its vital importance to Convention States in identifying and investigating cyberattacks, counter-espionage and terrorism. Suspicion in relation to those subjected to bulk surveillance is, therefore, not required.[275] The same goes for surveillance by law enforcement agencies should other means be insufficient to prove the involvement of specific individuals in serious crimes such as murder, armed robbery and crimes that has to do with extremism and major organized crime.[276] At the same time, the legislation:

> [C] annot be drafted in such vague terms as to leave room for speculation and assumptions with regard to its content and, most importantly, with regard to the person in respect of whom the measure is being applied.[277]

For this reason, the decision to authorize covert surveillance of a 'stabbing victim and his contacts' was considered too vague to comply with Article 8, according to the ECtHR.[278] As concerns collateral intrusions, where the conversation of third parties is intercepted accidentally in the course of a criminal investigation, the Court has not addressed the issue beyond stating in general terms that such measures are "particularly intrusive and that there is a need for safeguards in this domain."[279]

---

[272] This is justified by the fact that lawyers and public watchdogs cannot fulfil their democratic functions without their exchanges of information remaining confidential. See *Catt v. the United Kingdom*, § 123; *Michaud v. France*, § 118; *Vasil Vasilev v. Bulgaria*, § 90; *R.E. v. the United Kingdom*, § 131; *Dudchenko v. Russia*, § 104; *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, § 127.
[273] See *Roman Zakharov v. Russia*, §§ 260–262.
[274] *Centrum för rättvisa v. Sweden*, §§ 240–243.
[275] See *Big Brother Watch and Others v. the United Kingdom*, § 424; *Centrum mot rättvisa v. Sweden*, § 259.
[276] See *P.G. and J.H. v. the United Kingdom*, §§ 42–51; *Greuter v. the Netherlands*; *Coban v. Spain*; *Deveci v. Türkiye*, §§ 21–24.
[277] *Azer Ahmadov v. Azerbaijan*, § 71.
[278] See *Azer Ahmadov v. Azerbaijan*, §§ 66–76.
[279] *Privacy International and Others v. the United Kingdom*, § 45. Also see *Lambert v. France*, §§ 35–41; *Bosak and Others v. Croatia*, §§ 65–68.

5.2.3 Connection Between Allowed Means of Interception and the Intrusiveness of Surveillance Measures

In view of the risk that a system of covert surveillance may undermine democracy under the cloak of defending it, Convention States may not choose whatever surveillance measures they deem necessary in the fight against crime.[280] Depending on what surveillance technologies are employed and where and how they are used, surveillance may be more or less intrusive, the former requiring greater justifications and safeguards than the latter.[281] As a general rule, Convention States may not use more intrusive means than necessary to achieve the legitimate aim or aims in question. By reason of this, intrusive surveillance measures may not be deployed without compelling reasons to do so, which depends on the seriousness of the acts.[282] Surveillance measures that do not include information about the content of the target's communications are generally considered less intrusive than visual, electronic and acoustic surveillance as they reveal less intimate details about the person under surveillance.[283] That is to say, surveillance measures that only collect 'peripheral information' sought by the police, such as names, addresses, IP addresses and location data.[284]

The level of intrusiveness is, however, not only dependent on the technical means used for surveillance. As stressed by the Court on several occasions, the time, place and duration of surveillance measures have equal influence on the assessment.[285] Since there is a higher expectation of privacy at home than in public places where people knowingly or intentionally involve themselves in activities that may be recorded or reported in a public manner, surveillance in public areas is considered less intrusive than surveillance taking place in private places or vehicles.[286] In addition to this, the combination of surveillance measures used against a person also contributes to the intrusiveness of the operation as a whole. As noted by the Court most recently in *Ekimdzhiev and Others v. Bulgaria*, "communications data […] can be used to

[280] See *Centrum för rättvisa v. Sweden*, § 253.
[281] As for the differences in terms of level of protection, the Court has stated that not all of the Huvig/Weber criteria are relevant for less intrusive surveillance measures. As long as the national authorities meet the general requirements of legality, necessity and proportionality applicable to surveillance measures in general, the ECtHR is satisfied with the authority's assessment. See *Uzun v. Germany*, § 63, 66; *R.E v. the United Kingdom*, §§ 123–131.
[282] See amongst many others, *Dragojević v. Croatia,* §§ 84–102.
[283] See *Kopp v. Switzerland*, § 72; *P.G. and J.H. v. the United Kingdom*, §; *Uzun v. Germany*, § 66; *R.E. v. the United Kingdom*, §§ 129–130; *Centrum för rättvisa v. Sweden*, § 277; *Big Brother Watch and Others v. the United Kingdom*, §§ 363–364.
[284] See *Breyer v. Germany*, § 76; *Uzun v. Germany*, § 66; *Benedik v. Slovenia*, § 109.
[285] See *R.E. v. the United Kingdom*, § 130; *Breyer v. Germany*, §§ 94–96; *Big Brother and Others v. the United Kingdom*, § 342.
[286] See *P.G. and J.H. v. the United Kingdom*, § 57; *R.E v. the United Kingdom*, §§ 158–159.

paint an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who that person has interacted with."[287] Thus, when combined, the intrusion of several less intrusive surveillance measures can be just as invasive as more technically advanced measures despite the content of the data being encrypted.[288]

5.3 Limits to National Surveillance Law in Jurisprudence of the ECtHR: Tentative Conclusions and Unresolved Problems

This chapter has attempted to provide an overview of the scope of covert surveillance practices and privacy in ECtHR case law. Overall, the cases support the view that interference with individuals' private lives is against the Convention unless done to prevent threats to national security or a clearly defined category of serious crimes that pose a particular danger to life and health (i.e., threats to public security). In this weighing process, the Court attaches great importance to the rule of law and the proportionality of the interference, which is evident by their focus on procedural safeguards to prevent abuse of surveillance powers in the Huvig/Weber criteria. As the Court stated in *Roman Zakharov v. Russia*, compatibility with the rule of law requires protection against arbitrary interferences with privacy, which is only the case if "the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the 'interference' to what is 'necessary in a democratic society.'"[289] However, at a closer examination of the ECtHR's case law, inconsistencies in the Court's statements of principle can be found. When comparing cases such as *Malone* and *Association for European Integration and Human Rights and Ekimdzhiev* to cases such as *Centrum för rättvisa* and *Adomaitis v. Lithuania*, it seems like the Court has started to accept more serious privacy intrusions in relation to less serious crimes than before, with a smaller number of factual circumstances supporting the need for the interference, despite maintaining a front of upholding the same values as they did years ago.[290]

[287] *Ekimdzhiev and Others v. Bulgaria*, § 394. Also see *Centrum för rättvisa v. Sweden*, § 246.
[288] See *Big Brother Watch and Others v. the United Kingdom*, §§ 342, 363.
[289] *Roman Zakharov v. Russia*, § 232.
[290] In all of the cases, the Court reiterates similar statements of principles for surveillance. See *Malone v. the United Kingdom*, §§ 67–82; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, §§ 69–94; *Centrum för rättvisa v. Sweden*, §§ 246–253; *Adomaitis v. Lithuania*, §§ 83–90.

In addition, it is not very clear from the case law of the Court what is required for the Convention States to live up to the described surveillance criteria substantially, which will be discussed further in chapter 7. For now, it is sufficient to say that there is not much guidance in the Court's case law on *which* categories of people and *what* types of offences should be included in the Criminal Codes of the Convention States. What is clear, however, is that the Court does not accept state surveillance of European citizens under what conditions whatsoever. There has to be a reasonable proportion between the gravity of the interference and the aims pursued, meaning that the response of covert surveillance to a specific threat should neither be excessive to its aims nor used without a particular goal in mind to facilitate criminal investigations in general. To explain what this means more concretely, the Swedish draft proposal to increase state surveillance powers will be used as an example of the limits to the Convention States' margin of appreciation.

5.3.1 Proposed Changes to Swedish Surveillance Law in the Light of Article 8 ECHR

At this point, it is established case law that the rule of law requires that regulations have a certain amount of foreseeability. With that in mind, it is unclear whether the Swedish proposal to *extend the crime catalogue* for covert surveillance is compatible with the ECtHR's rule of law requirements, as they require a clear definition of the type of offences that can give rise to covert surveillance. While there is no obligation for the Convention States to set out the categories of crimes that may give rise to covert surveillance in an exhaustive list, the Court has made it clear that the list must be of such clarity that it can provide guidance on the nature of offences that may give rise to an interception order. Inherent in this understanding of foreseeability is the idea that citizens should be able to understand what type of criminal behaviour can give rise to surveillance, which is impossible if the law allows covert surveillance for an 'extensive range of criminal offences.'[291] Since the suggested penalty valve is formulated so that a combination of 'connected' crimes can give rise to surveillance, it is not unlikely that the Court would object to the proposal's vagueness as it essentially only excludes pecuniary offences.[292] Another problematic aspect of the proposal is that the envisaged crimes for surveillance are not that serious (theft, fraud, embezzlement etc.) and that it is hard to know

[291] See *Roman Zakharov v. Russia*, §§ 244–248.
[292] The reason for this is that the proposal only excludes crimes that cannot lead to a detention order (i.e., crimes with pecuniary punishment). Compare SOU 2022:19, 138–139 to 24:1 CPJ.

which combination of crimes can give rise to surveillance from reading the proposal.[293] That being said, it is questionable how predictable the penalty valve would appear to individuals, as it would be difficult for them to predict which kinds of behaviour might leave them susceptible to covert surveillance.

As for the types of offences that are *serious enough* to warrant privacy restrictions for crime-fighting purposes on their own merit, there is, as indicated above, no general benchmark for the seriousness required. The case law does seem to suggest that minor offences with little risk of endangering the public are not serious enough for the most intrusive surveillance measures, characterized by measures capable of recording and *intercepting* conversations.[294] In view of this and what was observed about the connection between the severity of a crime and the allowed intrusiveness of surveillance measures in sections 5.2.1-5.2.3, it can be assumed that the ECtHR would have some objections to the proposal in SOU 2022:19. As stated in section 3.2.1, the proposal to increase the use of secret interception of electronic communications, camera surveillance and data surveillance includes offences such as perjury, extortion and hunting violations. Since those crimes pose no immediate risk to health or public order, it is unclear whether they would be considered serious enough to give rise to an interception order with the amount of personal information sound - and image recording devices reveal about a person.

Turning to the crime catalogue for preventive surveillance measures in SOU 2022:52, it is not unlikely that the ECtHR would find the offences serious enough to warrant privacy restrictions as the list includes crimes that can hurt specific individuals and society if not prevented.[295] Nevertheless, it remains uncertain whether the Court would be satisfied with the safeguards against abuse, as the proposal targets innocent people without a concrete plan on how to minimize the risk of people at no danger of committing or having relevant information about crime from being targeted by the police.[296] Therefore, it can be assumed that the Court would object to the proportionality in removing the suspicion threshold for covert surveillance, which should also extend to pre-trial measures.[297] By formulating the requirements for pre-trial

[293] With the exception of the offences listed, the Inquiry Chair has left the question of which types of offences that might be covered by the proposal open, see SOU 2022:19, 131–137.
[294] See *Uzun v. Germany*, § 66.
[295] For example, murder, grave narcotics crime and destruction causing public endangerment. See part 3.2.1.
[296] Compare SOU 2022:52, 176–177, 201–227 to part 5.1.2 and part 5.2.2.
[297] The importance of procedural safeguards for the proportionality assessment is stated in, inter alia, *Breyer v. Germany*, §§ 97, 103; *Iordachi and Others v. Moldova*, §§ 48–52 Also see part 5.1.2 and 5.2.2.

'suspicionless surveillance' in such vague terms that virtually anyone could be a target of covert surveillance, irrespective of their own behaviour, it becomes nearly impossible to assess whether a fair balance has been struck between the target's interest of privacy and the law enforcement's interest in fighting crime. When the legislator has framed the legal framework as a regime of 'targeted surveillance', as is true for SOU 2022:19, the ECtHR has also explicitly expressed that criminal suspicion is required, except for the most serious crimes of violence.[298] Since many of the offences listed in the crime catalogue are non-violent, it is doubtful whether all violations would be considered serious enough to warrant suspicionless surveillance.

In terms of the degree of risk or suspicion required for preventive surveillance measures, it is more difficult to predict the reasoning of the ECtHR. While the Court has made it clear that covert surveillance for national security purposes performed by intelligence services does not require reasonable suspicion, it has remained silent on the issue of suspicion in relation to policiary investigations that fall somewhere in between the area of criminal intelligence and national intelligence, which is the case for SOU 2022:52, as the proposal sets out to "expand the use of existing preventive coercive measures at the intelligence stage [own translation]" by giving law enforcement agencies more effective tools to "prevent serious crimes outside of criminal investigations [own translation]."[299] Without knowing the ECtHR's stance on hybrid investigations, it is therefore not possible to come to any conclusions about their permissibility since they are blurring the line between preventive bulk surveillance and crime-solving targeted surveillance.

Lastly, when it comes to the proposal to allow *personalised instead of location-based covert surveillance*, it is difficult to conclude its compatibility with Article 8 ECHR. The main challenge with the proposal from a privacy standpoint is the increased risk of collateral intrusions, as the proposal would make it easier to place hidden cameras and mikes in public places, which increases the risk of unintentional interference with the privacy of bystanders. An example would be the accidental recording of background information in local meeting places or, as suggested in the proposal, 'collateral persecution of individuals' movements through secret camera surveillance with drones.'[300] Whether the increased risk of collateral intrusion would be tolerated depends on an overall assessment of the potential advantages and

[298] See part 5.2.
[299] SOU 2022:52, 179.
[300] SOU 2022:19, 338–339.

disadvantages of the proposal. Since there are already CCTV cameras in public places,[301] and surveillance in public areas is not considered as intrusive as surveillance in private homes and vehicles, it is not unlikely that the ECtHR would consider the proposal within Sweden's margin of appreciation.[302] At the same time, the Court is generally negatively disposed to the initiation of interception processes without "due regard to the corresponding level of intrusion into the Convention rights of the persons likely to be affected."[303] If the opportunity to tie surveillance permits to specific individuals would be utilized frivolously without properly considering the impacts of the surveillance on others and whether the information would be beneficial to the investigation, the Court would probably not consider the surveillance that necessary or proportionate.

5.3.2 Concluding Remarks and Questions Left Unanswered by the Court

To conclude this chapter, it can be established that the ECtHR's approach to covert surveillance has changed over the years with an increased threat to internal and external state stability, which partly has been accelerated by new sophisticated communication devices and the development of technology in general. When reviewing the compatibility of the Convention State's regulations on covert surveillance, the state's interest in protecting its citizens from threats is constantly present, sometimes to the point of overshadowing the interest of protecting privacy for the sake of individual integrity or democracy-enhancing reasons. Or at least that is how it appears from reading the Court's judgements, as the balancing parts of the decisions are often not that detailed, except when it comes to the passages on generally applicable surveillance principles. The level of scrutiny by the Court in covert surveillance cases has also tended to fluctuate in its strength, going back- and forward between the number of necessary safeguards in relation to covert surveillance and the appropriate amount of criminal suspicion required for targeted surveillance cases on the one hand, and untargeted surveillance cases on the other hand.

As the case law stands now, the Huvig/Weber criteria seem applicable to targeted surveillance, while the criteria developed in *Big Brother Watch* and *Centrum för rättvisa* seem to apply to bulk surveillance.[304] If the means for targeted surveillance is not that intrusive in itself and can only provide limited details about the target's location data or other types of more 'peripheral

[301] See generally, Polismyndigheten, 'Polismyndighetens kamerabevakning av platser dit allmänheten har tillträde'.
[302] See part 5.2.3.
[303] *Centrum för rättvisa v. Sweden*, § 270.
[304] See part 5.2.2.

data', some of the Huvig/Weber criteria might not even be relevant for the assessment.[305] Which standards apply under what conditions still remain unclear, as does the question of how likely it must be that the surveillance has a positive outcome for the criminal investigation at hand for it to be initiated, which is problematic from a legitimacy standpoint as:

> Effectiveness and accuracy are intrinsically linked to ethics and legality: if it cannot be demonstrated that a particular tool or method is operating effectively and with a reasonable degree of accuracy, it may not be possible to justify the use of such a tool as necessary to fulfil a particular policing function.[306]

With this in mind, the next chapter will explore the justifications for war in JWT to see if the ethical framework for just warfare can clarify what is meant by proportionate surveillance and how it can be conducted in a way that is foreseeable enough to be democratically transparent and efficient enough to counter serious threats to society.

[305] See footnote 281.
[306] Babuta and Oswald, 'Data Analytics and Algorithmic Bias in Policing', 5. Although the paper is about the use of analytics and algorithms for policing, the same reasoning should apply to other technological means used by the police as they fulfil similar functions, i.e., the detection, prevention and prosecution of criminal offences.

6 Proportionality under Article 8 ECHR and Just War Principles – What is the Lesson to Be Learned?

Just as the principles of legitimacy, necessity, and proportionality specify the scope and permissibility of surveillance practices under article 8 ECHR, IHL specify the conditions wars must meet to be justified. As a set of rules, IHL aims to balance humanitarian concerns with military necessity by setting out restrictions on the means and methods of warfare.[307] The customs of warfare, as set out in the Charter of the United Nations[308], the Hauge Regulations[309], the Geneva Conventions[310] and its Additional Protocols[311], have universal acceptability for the most part.[312] An overview of the applicable principles can be found in the International Committee of the Red Cross (ICRC) study on customary IHL, which consists of customary rules accepted as law independent of their codification in international treaties.[313] There are generally two distinct aspects of proper warfare in just war tradition. The first, known as *Jus ad Bellum*, specifies the conditions under which the resort of war is morally justified. The second, known as *Jus in Bello*, regulates what is permitted in battle.[314] Together they create the seven founding principles of JWT: the principle of just cause, right authority, right intention, last resort, proportional means, discrimination and reasonable prospects.[315]

[307] See Steinhoff, *On the Ethics of War and Terrorism*, 2–3.
[308] Chapter 1, Article 2(4); chapter 7, Article 51, chapter 7, Article 42.
[309] Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907; Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 29 July 1899.
[310] Convention I: Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Geneva, August 12, 1949; Convention II: Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Geneva, August 12, 1949; Convention III: Treatment of Prisoners of War, Geneva, August 12, 1949; Convention IV: Protection of Civilian Persons in Time of War, Geneva, August 12, 1949.
[311] Additional Protocol II: Protection of Victims of Non-International Armed Conflicts, June 8, 1977; Additional Protocol III: Adoption of an Additional Distinctive Emblem, December 8, 2005.
[312] All treaties, except for the Additional Protocols to the Geneva Conventions, have been universally ratified. See ICRC, 'Treaties, States Parties, and Commentaries - States Parties - Convention (IV) Relative to the Protection of Civilian Persons in Time of War. Geneva, 12 August 1949.'; UN, 'United Nations Treaty Collection'.
[313] See ICRC, 'ICRC's Study on Customary International Humanitarian Law (IHL)'; ICRC, 'Customary Law'.
[314] Steinhoff, *On the Ethics of War and Terrorism*, 2–3.
[315] See International Commission on Intervention and State Sovereignty et al., *The Responsibility to Protect*, 32. Although there is no universally accepted list of just war principles, the criteria of the Commission are often used to describe the founding principles of IHL and JWT. E.g., McMahan, 'Just War', 670; Steinhoff, *On the Ethics of War and Terrorism*, 1.

6.1 The Justification of Using JWT as a Starting Point for Designing an Ethical Framework for Covert Surveillance

Virtually every ethical system reflects the basic principle that the deliberate taking of human life is morally wrong. At the same time, intentional killing and violence can be the less evil alternative in some circumstances, like war, when the decision to abstain from using force might result in mass destruction, death and the loss of state sovereignty. To a specified degree, it is therefore 'acceptable' to engage in morally questionable actions for a just cause.[316] JWT has consequently emerged as a potential ethical framework for covert surveillance, as both practices involve reconciling the "tension that is born from balancing the needs of the political community with the harm the protection of those needs can cause for the individual."[317] Just like war involves practices contrary to the moral rules that govern most human activity, covert surveillance cannot, at least in some respects, be conducted efficiently without cutting across normal expectations of morality.[318] In this case, the violation of the expectation of privacy. To access information about a person without consent is highly controversial as most people expect information about themselves not voluntarily disclosed to stay private.[319]

Like war, surveillance practices can also result in collateral damage. That is accidental damage to civilians without connection to criminality or war.[320] Yet, most would agree that there are cases in which covert surveillance is justified. For example, to prevent a public shooting or to catch a murderer.[321] Since JWT tries to minimize humanitarian suffering in war by prohibiting the kind of excessive violence that would inflict collateral damage to civilians,[322] more could be learned about the proper scope of covert surveillance by applying JWT to surveillance practices. This is by considering whether there is a specific just cause for the operation and whether the chosen method is proportionate to its proposed gains.[323]

---

[316] See Coverdale, 'An Introduction to the Just War Tradition', 4, 7.
[317] Bellaby, 'Justifying Cyber-Intelligence?', 304.
[318] See Quinlan, 'Just Intelligence', 3, 6.
[319] See Rengel, *Privacy in the 21st Century*, 30.
[320] When offenders violate the law, they create a number of explicit and implicit relationships between victims, witnesses, and other innocent people, such as family and friends, who may be mistaken for the real offender. Innocents may also be subject to surveillance accidentally by communicating with the suspect while he or she is under surveillance. Collateral damage therefore occurs when the privacy of innocent individuals is compromised as the result of a criminal investigation, and sensitive information is therefore accidentally disclosed. See Utset, 'Digital Surveillance and Preventive Policing', 1464; Choo and Sarre, 'Balancing Privacy with Legitimate Surveillance and Lawful Data Access', 9.
[321] See Macnish, 'Surveillance Ethics', 9.
[322] See Schulzke, *Just War Theory and Civilian Casualties*, 3.
[323] See Bellaby, 'Justifying Cyber-Intelligence?', 305.

Certain drawbacks are, however, associated with using JWT as a normative framework for covert surveillance practices. As noted by several critics, surveillance is not warfare. At its core, policing is about maintaining internal stability, and war is about physical coercion (i.e., taking life, destroying property, etc.). Applying JWT to covert surveillance could therefore be seen as illogical, as police surveillance seeks to save lives, not take them. Surveillance, unlike warfare, thus is not so morally reprehensible that it needs to be avoided at all costs. On the contrary, intelligence collection is often the first step in a chain of increasingly intrusive security measures as it is considered least harmful to the individual.[324] While it is true that surveillance harms are less obvious than war injuries and that the use of JWT cannot be justified solely on the grounds that surveillance, just like war, must have a just cause or be proportionate,[325] the fact remains that there are few other theories equipped to deal with complex security issues.[326] Not at least with such a rich philosophical tradition as JWT.[327] Therefore, as mentioned at the beginning of the essay, JWT is the most appropriate starting point in designing an ethical framework for surveillance practices.[328]

6.2 Principles of Just Surveillance

The principles of just surveillance, as most famously advocated by Bellaby, Macnish, Omand and Phytian, can be summarized as follows.[329] For surveillance to be justified, it should be undertaken for a just cause.[330] In this case, the protection of public security since it is the police's responsibility to serve people and communities by maintaining public order and combating crime.[331] Moreover, the *principle of just cause* requires the existence of a sufficient threat that can justify the harms of surveillance. The more harmful the surveillance act is, the greater threat and evidence of said threat is required to justify the intervention.[332] The intention behind subjecting a target to surveillance should also be the same as the cause given for

[324] See Miller, Regan, and Walsh, *National Security Intelligence and Ethics*, 25; Auten, 'Examining Just Intelligence Theory'; Stoddart, 'Challenging "Just Surveillance Theory"', 162; Miller, 'Rethinking the Just Intelligence Theory of National Security Intelligence Collection and Analysis', 216.
[325] See Fabre, *Spying through a Glass Darkly*, 24–25. Also see chapter 4, which thoroughly describes the dangers of surveillance to democracy.
[326] As noted by Bellamy, no other theory reflects the inherent tension between what is good for society and what is good for the individual as well as JWT. See Bellaby, 'What's the Harm?', 109.
[327] See Hosein, 'On Just Surveillance', 154; Macnish, 'Just Surveillance?', 152.
[328] See section 1.4.
[329] Their most famous work include: Omand and Phythian, *Principled Spying*; Bellaby, 'What's the Harm?'; Macnish, 'Just Surveillance?'
[330] Salacious, trivial or ignoble causes such as the protection of pride does not count, Macnish, 'Just Surveillance?', 147.
[331] See ICRC, 'International Rules and Standards for Policing', 18.
[332] See Bellaby, 'What's the Harm?', 109.

surveillance according to the *principle of right intention*. Should the police pursue a different end, they would not meet the requirement. Prohibited intentions include using public security as a smokescreen for political, economic and social objectives, using camera surveillance to identify attractive members of the opposite sex instead of suspected terrorists and listening in on phone calls that have nothing to do with the crime under investigation.[333]

Another cornerstone of JWT is the *principle of right authority*, according to which war must be authorized by the right authority for it to be permissible. Traditionally, that role is reserved for the state or the government since the legitimate authority must have certain moral and legal capabilities. A legitimate authority holds the political and moral power necessary to wage war. It acts not on behalf of its own interest but on behalf of those who have agreed to transfer their rights to the state through law.[334] Thus, for surveillance to be morally permissible, it must be authorized by the right authority in more than one capacity. Besides making sure that the surveillance has a basis in domestic law, the principle demands that the law itself is sufficiently accessible so that the manner in which it operates, or is applied, is foreseeable to the public. The legitimate authority criterion also applies to those acting on behalf of the state. All surveillance measures must therefore be authorized by the proper national authority and be subject to external oversight.[335]

The *principles of last resort, proportional means and reasonable prospects* attempt to limit the potential negative consequences of surveillance practices by weighing the potential costs and benefits of the proposed measures. Before any surveillance measures are taken, less harmful means should have been attempted. The *last resort principle* does not necessarily mean that surveillance is the last step in a chronological series of actions. What it means is that surveillance should not be used out of ease, efficiency or expediency when other less harmful means could have achieved the same outcome.[336] For surveillance to be acceptable, there must also be a reasonable prospect of success. If the surveillance operation is unlikely to result in evidence of use for the investigation, it should not be initiated in the first place. Having adequate

[333] See Macnish, 'Just Surveillance?', 148; Bellaby, 'Justifying Cyber-Intelligence?', 306; Bellaby, 'What's the Harm?', 112.
[334] See Coates, *The Ethics of War*, 142; Bellaby, 'Too Many Secrets?', 82; Besser-Jones, 'Just War Theory, Legitimate Authority, and the "War" on Terror', 141–42.
[335] See Omand and Phythian, *Principled Spying*, 81; Bellaby, 'What's the Harm?', 110–11.
[336] See Bellaby, 'Too Many Secrets?', 80.

justification for surveillance based on probabilistic reasoning prevents general 'fishing expeditions' in the hope that the guilty party will be found if enough people are investigated.[337]

The question of legitimate targets arises again in the *principle of discrimination*, which will be developed further in part 6.3. In short, the *principle of discrimination* requires that a distinction be made between legitimate and illegitimate surveillance targets. Just as soldiers waive their protective rights by acting in a threatening way in JWT, suspects of crime can become legitimate targets by way of their actions.[338] In the context of law enforcement, appropriate targets would be those guilty of threatening security or of criminal acts, and inappropriate targets people innocent of such actions. However, since surveillance is often carried out to re-enforce evidence of guilt and usually takes place in the presence of others than the suspect, surveillance of innocents cannot be avoided altogether. For that reason, just surveillance principles accept some collateral damage as long as reasonable efforts are made to minimize the risk to innocents.[339]

Lastly, to satisfy the *principle of proportionality*, the ethical risks of the operation must be in line with the harm that the operation is intended to prevent. The authorizer has to judge not only the potential risks with the operation but also what risk is represented by not conducting the operation.[340] According to Bellaby, the assessment should always include a calculation of the overall damage caused by the operation to the targeted individual as well as the damage to society. Such damage includes damage to social cohesion, degradation of trust between social groups, aggregation of minor harms into larger harms and the potential for radicalisation.[341] It should also be noted that some surveillance measures are more intrusive than others. Types of surveillance which collect and record content are generally more intrusive than those that collect and record metadata. Thus, it might be proportionate to subject a person actively engaged in a terrorist plot to wiretapping or email monitoring, while such measures would be disproportionate in relation to, say, minor tax fraud or theft, considering the amount of

[337] See Omand and Phythian, *Principled Spying*, 80,82; Macnish, 'Just Surveillance?', 150.
[338] See Bellaby, 'What's the Harm?', 116.
[339] See Omand and Phythian, *Principled Spying*, 83; Macnish, 'Just Surveillance?', 151.
[340] See Omand and Phythian, *Principled Spying*, 79–80.
[341] See Bellaby, 'Justifying Cyber-Intelligence?', 308.

information disclosed about the person.[342] Likewise, it would be disproportional to bug all the phones in an area with frequent car theft instead of installing CCTV cameras.[343]

6.3 Additional Safeguards to Non-Suspects

Despite emphasising the importance of proportionality in covert surveillance practices, neither just surveillance principles nor the ECtHR really addresses the proportionality in subjecting innocents to covert surveillance, which is problematic considering the effects of surveillance on democratic self-governance.[344] The ambiguity of rules governing surveillance practices has not gone unnoticed by practitioners and scholars. To quote Brown and Korff, "[t]he definitions of […] general 'grounds for suspicion' […] that are felt to justify police action – are becoming increasingly vague" [345] in lack of clear legal standards developed by international courts and other influential bodies such as the UN. In *Big Brother Watch and Others v. the United Kingdom*, the dissenting judges even went as far as to accuse the majority of opening the gates for an electronic 'Big Brother' in Europe because of their new relaxed approach to bulk surveillance not dependent on reasonable suspicion.[346] Despite maintaining that reasonable suspicion is an important safeguard in relation to targeted surveillance operations,[347] the ECtHR does not address whether so-called 'hybrid investigations' where there is an overlap between traditional intelligence powers and law enforcement powers require reasonable suspicion.[348] As noted by judge Pinto de Albuquerque, the Court's position in *Big Brother Watch* leaves many questions unanswered. One is the necessary degree of interest in individual communications for 'identifying and preventing threats to essential national interests.'[349] One way to look at it, as suggested by Rønn and Lippert-Rasmussen and Nathan, is to view surveillance as a form of self-defence that can only be proportional when the targets have made themselves 'liable' to

[342] As Macnish writes on page 26 in 'An Eye for an Eye', such measures "might give indications that the person is having an affair, that they have particular medical problems, or even that they are contemplating suicide, depending on where they are, and for how long, if they have their mobile phone with them." Also see Macnish, 'An Eye for an Eye', 13.
[343] See Macnish, 'Just Surveillance?', 151.
[344] Some examples of such consequences can be found in chapter 4.
[345] Brown and Korff, 'Terrorism and the Proportionality of Internet Surveillance', 126.
[346] See Joint partly concurring opinion of Judges Lemmens, Vehabović and Bošnjak, §§ 3–10, 15, 20, 30; Partly concurring and partly dissenting opinion of Judge Pinto de Albuquerque, §§ 22–23, 58–59.
[347] *Big Brother Watch and Others v. the United Kingdom*, § 348.
[348] Since the main purpose of intelligence collection is to prepare for and prevent threats to the state and its population, intelligence services do not usually hold law enforcement powers such as powers of arrest, detention and interrogation. See DCAF, *Counterintelligence and Law Enforcement Functions in the Intelligence Sector*, 2020:2; DCAF, *Intelligence Services Roles and Responsibilities in Good Security Sector Governance*, 2015:2.
[349] Compare the majority's view in *Big Brother Watch and Others v. the United Kingdom*, § 340 to § 14, Partly concurring and partly dissenting opinion of Judge Pinto de Albuquerque.

preventive harm.[350] That is to say, when a person is implicated in a threat to public security in such a way that harming him in the course of preventing that threat would not wrong him.[351]

6.3.1 What Does It Take to Become Liable to Covert Surveillance?

How does a person innocent of crime become liable to covert surveillance? In Rønn and Lippert-Rasmussen's view, liability is connected to the principle of discrimination in JWT. The more disconnected a person is from a crime, the less proportionate it is to subject him or her to surveillance, as surveillance always involves some harm to the individual. When surveillance is inflicted upon an individual that the authorities believe is a threat to public security, the intrusion can be justified as self-defence, provided that the degree of intrusion imposed upon the threatener is not greater than the threat itself.[352] By taking part in conduct that might harm others, the attacker has forgone his right not to be injured, as states are allowed to use force in self-defence to overcome a culpable threat. Extending this to legitimate police action, one might say that threatened criminal activity is necessary to establish liability.[353] How much harm is proportionate to fend off a threat relies on the nature and degree of damage inflicted upon the threatener, together with his degree of involvement in the threat. Just as a higher degree of participation in war makes a combatant liable to a greater self-defensive force in JWT, so does a higher degree of liability make a criminal subjectable to more intrusive or harmful surveillance practices.[354] Surveillance of non-liable individuals therefore requires more justification than surveillance of liable individuals since they "are neither blameworthy nor implicated in the existence of the problem […] potentially solved by" [355] surveillance.

6.3.2 The Difference Between Wide and Narrow Proportionality

To capture the difference between being liable and not liable to defensive harms, Rønn and Lippert-Rasmussen distinguish between intentional and unintended but foreseeable intrusions upon liable and non-liable individuals (i.e., wide and narrow proportionality). In their view, there is a lesser burden of justification when the target of the surveillance is liable or when the intrusion of an innocent person's privacy is foreseen but unintended – the main difference being the intention behind the targeting. The intentional targeting of non-liable individuals most

[350] See Nathan, 'Liability to Deception and Manipulation', 370; Rønn and Lippert-Rasmussen, 'Out of Proportion?', 1.
[351] See Rønn and Lippert-Rasmussen, 'Out of Proportion?', 8.
[352] See Rønn and Lippert-Rasmussen, 10–11, 20.
[353] See Nathan, *The Ethics of Undercover Policing*, sec. 1 The Liability View.
[354] See Nathan, 'Liability to Deception and Manipulation', 374.
[355] Rønn and Lippert-Rasmussen, 'Out of Proportion?', 10.

closely resembles what the ECtHR calls bulk surveillance. The resemblance is most suitable because this type of surveillance does not require individualized suspicion. As Rønn and Lippert-Rasmussen write, mass surveillance is characterized by "wide collections of personal electronic pieces of information in the name of general crime and terrorism prevention."[356]

In these cases, the target of the surveillance is not involved in any criminal wrongdoing but is used as a means of acquiring information that might be useful for mitigating threats to public security. Similar to the draft proposal by the Swedish Government mentioned in Part 3.2.2, the connection to the security threat is not liability but proximity (friendship, kinship, work relations etc.). Thus, the intention behind the surveillance is not to gather personal information about the targets per se but to learn more about a threat to public security by collecting information from those closest to the perceived threat to learn more about its danger to society.[357] A similar but slightly different situation would be the foreseen but unintended collection of information on people caught in communication with the legitimate target (i.e., collateral intrusions).[358] The intrusion upon the lives of innocents on such occasions is unwanted but nevertheless expected since it cannot be ruled out that a tap on a telephone or a bugging device installed in a vehicle will pick up innocent conversations with family members or third parties.[359] The intention of the operation is, however, not to monitor the activities of relatives but to monitor the activities of the liable.

While surveillance of non-liable individuals cannot be defended as self-defence in the classic sense, as they have not waived their protective rights, the surveillance can be justified on the grounds that subjects have *ceded* some of their rights by associating with the threat. One could say that the risk of imposing or facilitating harm generates some duty to cooperate with the police, even if the contribution to the threat is unknown to the individual.[360] How far that 'duty' extends depends on to what extent the expected goods of the intrusion outweigh the harms. In contrast to narrow proportionality, which presumes that surveillance is legitimate as long as the positive effects of the surveillance outweigh the harms inflicted upon the liable, wide proportionality is judged according to the doctrine of *lesser evil justifications*, in which the pertinent factor in terms of proportionality would be that the intrusion upon the non-liable

[356] Compare Rønn and Lippert-Rasmussen, 19 to B*ig Brother Watch and Others v. the United Kingdom*, § 326.
[357] See Rønn and Lippert-Rasmussen, 14.
[358] See Rønn and Lippert-Rasmussen, 12, 14.
[359] See Omand and Phythian, *Principled Spying*, 24.
[360] See Nathan, 'Liability to Deception and Manipulation', 377.

would cause the avoidance of a greater intrusion upon non-liable individuals.[361] Accordingly, the threat to the public to be prevented must be significantly more serious than the expected harm to the surveillance target for the surveillance to be justified. This is especially true when it comes to planned intrusions, as there is no connection between guilt and targeting in those cases.[362] On this view, it is clear that only particularly serious crimes with some risk of immediate harm or urgency should be able to give rise to surveillance.[363] Following this understanding of a threat, it is also questionable whether bulk surveillance for the purposes of general crime prevention is proportionate, as the surveillance does not lead to the avoidance of a specific threat in those cases.[364]

6.4 The Legitimacy of Surveillance in JWT and ECtHR Case Law

Having pointed out the main features of the comparative approaches to covert surveillance in JWT and the case law of the ECtHR, it is clear that there are some divergences between the two frameworks. Perhaps most noticeable in relation to the different requirements for suspicion, where JWT has a slightly higher threshold for surveillance than the ECtHR because of the emphasis on discrimination in JWT. The most significant difference between the two frameworks is, however, not the substance of the frameworks but which elements of the proportionality assessment are highlighted.[365] Whereas JWT is more concerned with the justifications for undertaking surveillance and its continued relevance for the investigation, the ECtHR is more concerned with the existence of procedural safeguards and judicial review. When the Conventions States have had procedural safeguards in place, the actual necessity and proportionality of the surveillance have been treated as secondary issues.[366] In *Kennedy v. the United Kingdom*, which concerned the alleged monitoring of a previous convict's communications without indications of a re-lapse into crime, the Court even went as far as to declare the question of whether the intrusion was necessary from a policiary point of view as

[361] See Vrist Ronn, 'Intelligence Ethics', 11, 15; Nathan, *The Ethics of Undercover Policing*, sec. 2 Proportionality.
[362] This is different from cases of collateral intrusions, where the connection between liability and targeting exists between the primary target (the suspect) and the threat that the primary target has created through his conduct.
[363] See Nathan, 'Liability to Deception and Manipulation', 380, 383.
[364] See Rønn and Lippert-Rasmussen, 'Out of Proportion?', 19.
[365] Both frameworks, for example, assesses the legitimacy of covert surveillance by looking at the declaration of intent for conducting surveillance, the necessity of the surveillance to achieve vital societal objectives and the proportionality of the surveillance in comparison to its damage to individuals. See chapters 5 and 6.
[366] See e.g., *Roman Zakharov v. Russia*, §§ 247–248; *Coban v. Spain; İrfan Güzel v. Turkey*, §§ 78–89; *Ben Faiza v. France*, §§ 77–80.

redundant, as the legal framework concerning covert surveillance was said to be able to provide 'sufficient safeguards' if such measures were in fact applied to the applicant.[367]

6.4.1 Required Burden of Proof under JWT and Article 8 ECHR

With the previous section in mind, an advantage that JWT has over Article 8 ECHR is that it provides more detail on what is required of nation-states to justify their need for covert surveillance substantially. While the ECtHR frames the necessity of surveillance measures as a question of 'relevant and sufficient reasons for surveillance', JWT demands actual proof of necessity.[368] For covert surveillance to be acceptable under JWT, the deciding authority has to show that there are reasonable grounds for believing that covert surveillance would be an effective step in mitigating an identifiable threat to public security and that it will continue to do so throughout the investigation. This is preferable from a rule of law perspective because it forces the authorising authority to go into the specific details of *why* covert surveillance is necessary to mitigate a particular threat and *why* it cannot be conducted by other less intrusive means, which promotes transparency and non-arbitrariness. The more detailed the requirements for initiating covert surveillance are, the harder it becomes for domestic authorities to use public security as a smokescreen for achieving unlawful objectives, as it makes it easier to identify divergences between the alleged and actual purpose of the investigation.

6.4.2 Foreseeable Application of Surveillance Laws – Discrimination is Key

Another lesson that the ECtHR could learn from JWT is how to distinguish between lawful and unlawful targets of surveillance more foreseeably, as the Court's case law has not been particularly forthcoming in that area.[369] As briefly discussed in chapter 4, foreseeability is one of the most important aspects of the rule of law. The Venice Commission defines foreseeability as the law being "formulated with sufficient precision and clarity to enable legal subjects to regulate their conduct in conformity with it."[370] To achieve such clarity in terms of who can be subject to covert surveillance and under what circumstances, discrimination is key. This is

[367] See *Kennedy v. the United Kingdom*, §§ 5–7, 155–170. It should be noted that this is not a critique of the Court's reasoning in the Kennedy judgement specifically, but a critique of the reluctance of the Court to address questions of strict necessity in general.
[368] For example, crime patterns over time, statistics, received intelligence from Security Services at home and abroad and information obtained through external sources and reconnaissance by the Police.
[369] As have been noted before, the case law of the ECtHR is not very clear on the subject of which persons may legitimately be subjected to secret surveillance in a state governed by the rule of law. See parts, 5.2.2, 5.3 and 6.3.
[370] European Commission on Democracy through Law (Venice Commission), *Rule of Law Checklist Adopted by the Venice Commission at its 106th Plenary Session (Venice, 11-12 March 2016)*, CDL-AD (2016)007, Strasbourg, 18 March 2016, 25.

because discrimination teaches us who is a legitimate and illegitimate target of surveillance by differentiating people based on their *immoral behaviour.* In a criminal context, the ability to anticipate the consequences of one's actions becomes even more essential as foreseeability is connected to the nullum crimen sine lege principle.[371] Although the principle has several meanings, the central message of the principle is that "no conduct shall be held criminal unless it is specifically described in the behavior-circumstance element of a penal statute."[372]

Like the presumption of innocence, the principle of nullum crimen sine lege acts as an important reminder of the role of foreseeability in a police state under the rule of law by giving expression to the notion that "[r]ules and practice concerning the required proof [*during criminal proceedings*] have to be clear and fair."[373] Fixed rules constrain government power by ensuring that state officials and others in power act according to the law and not according to their own beliefs, prejudices, career interests or other factors that affect human decision-making. By holding state officials accountable to the law, the rule of law installs trust in state institutions and democracy by reassuring citizens that they are free to do and act as they like as long as they follow the law and respect the 'social contract.'[374] When the state subjects innocents to coercive measures, it violates the citizen's confidence and shows a lack of respect for personal autonomy by treating citizens as means to achieve a goal rather than as human beings deserving of being treated with dignity.

The presumption of innocence also contains an element of proportionality. As the threat to the defendant's bodily autonomy and liberty becomes more serious, the standard of proof in traditional criminal law rises, which can be demonstrated by the different burdens of proof for seizes and searches, detention and prosecution. The reasoning behind this is that guilt, and ultimately conviction, will justify these deprivations of liberty in the end and that the state should avoid inflicting injury until it can be established that it can be justified.[375] JWT reflects this way of viewing legitimate state power as it considers the likelihood that an individual will pose a threat to society (i.e., their grounds for suspicion), together with the gravity of the

[371] See Venice Commission*, Rule of Law Checklist Adopted by the Venice Commission at its 106th Plenary Session (Venice, 11-12 March 2016)*, 27.
[372] Hall, 'Nulla Poena Sine Lege', 165. Also see Fellmeth and Horwitz, 'Nullum Crimen Sine Lege'.
[373] Venice Commission, *Rule of Law Checklist Adopted by the Venice Commission at its 106th Plenary Session (Venice, 11-12 March 2016)*, 44.
[374] See parts 4.2.1 and 4.3.
[375] See Ferguson, 'The Presumption of Innocence and Its Role in the Criminal Process', 150–51; Wilkinson, 'THE PRESUMPTION OF CIVIL INNOCENCE', 603–4.

suspected crime, when assessing the proportionality in subjecting a person to surveillance measures. From a proportionality perspective, this is preferable to the ECtHR's more lenient approach to evidence of guilt as it reduces the risk of people being subjected to unwarranted privacy intrusions by promoting restraint of power and objectivity.

7 Analysis: Surveillance and the ECHR – Are Covert Practices in Line with Democratic Society?

From a state point of view, it is understandable why proactive policing has become so popular. Confronted with increased threats of organised crime, drug trafficking and terrorism, it is only natural that countries such as Sweden have started to undertake measures to improve public protection as it is their duty to 'deter the commission of offences that threaten the right to life by setting up a law-enforcement machinery capable of preventing, suppressing and sanctioning such breaches.'[376] The securitisation rhetoric also appeals to the electorate as it gives them the impression that the state has control over the situation and is doing everything in its power to deal with the crisis at hand.[377] Still, there is a danger with defending security measures aimed at managing risks before they manifest with the motivation that it 'saves people from becoming victims of a crime in the future', as it lulls people into a false sense of security. Even if increased surveillance measures would reduce crime, which some scientists and scholars dispute,[378] increased security does not equal increased liberty. When the net is cast too wide, and the number of people of interest for covert surveillance encompasses everyone potentially threatening the public, it is hard to uphold the belief that 'what the government does to *others* does not apply to *us* law-abiding citizens.'[379] As has been argued by Waldron and Lazarus, there is a risk that we become so preoccupied with delivering security that we end up with perfect security and very little liberty.[380] This raises the question of whether the European privacy framework can balance these competing interests and, more importantly, whether it can do so without cutting across core democratic principles.

7.1 The ECtHR and the Rule of Law

On the face of it, there is no problem with ECtHR's jurisprudence on privacy from a rule of law perspective. With the Court's focus on procedural safeguards in the Huvig/Weber criteria, it should be quite the opposite. Yet, as illustrated in chapter 6, some weaknesses in the ECtHR's rule of law requirements for secret surveillance can be found as concerns the categories of people who can be subjected to surveillance under Article 8 ECHR. As the existence of criminal

[376] See *Osman v. the United Kingdom*, § 115.
[377] As Garland writes, "A show of punitive force against individuals is used to repress any acknowledgement of the state's inability to control crime to acceptable levels [*and*] a failure to deliver security to the population at large." See Garland, *The Culture of Control*, 114.
[378] See part 7.1.2.
[379] See Maras, 'The Social Consequences of a Mass Surveillance Measure', 68.
[380] See Waldron, *Torture, Terror, and Trade-Offs*, 166; Lazarus, 'Positive Obligations and Criminal Justice', 151.

suspicion also impacts the necessity and proportionality of surveillance measures,[381] the following sections will elaborate on the importance of suspicion for the legitimate use of police power. Only, this time, with a focus on the advantages and disadvantages of using liability instead of criminal severity as a justification for covert surveillance.

7.1.1 Liability vs Seriousness of the Threat

Before discussing the advantages and disadvantages of the different approaches to suspicion and 'civilian casualties' under JWT and Article 8 ECHR, it is important to remember that none of the regulations prohibits 'suspicionless' surveillance. While neither of the frameworks is particularly favourably disposed to interferences with privacy without prior suspicion, the rules are based on a pragmatic view of legitimate state power in which some collateral damage to innocents must be tolerated in the exercise of coercive powers. As the ECtHR noted in *Klass v. Germany*:

> Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction.[382]

In the interest of effective law enforcement, the interest of personal integrity has therefore had to take a step back, as it would be impossible to use these types of technologies if all accidental intrusions were prohibited. As noted, it is impossible to know whether someone irrelevant to the investigation might walk by an area under camera monitoring or if the communication of a family member or acquaintance will be intercepted by accident when monitoring a suspect's phone calls. That being said, it can be concluded that there is a place for pre-emptive surveillance measures in a democratic society. To what extent such measures are accepted depends on the regulatory framework consulted. While JWT is principally opposed to intentional privacy intrusions upon non-liable individuals, the ECtHR seems more inclined to accept such infringements, provided that the national authorities can demonstrate the need for such measures convincingly enough. That is to say, if the crime under investigation can be viewed as a 'serious offence.'[383]

[381] Which, incidentally, also constitute important elements of the rule of law, see part 4.3.1.
[382] *Klass v. Germany*, § 48. That such measures also include preventive surveillance powers can be deduced from the judgements of *Deveci v. Türkiye*, *Greuter v. the Netherlands* and *Coban v. Spain* (see part 5.2.2).
[383] See part 5.2.1

The risk with such a 'relaxed' approach to suspicion and necessity is that concerns about personal integrity get lost in the 'immense benefits of such measures to society.' If states start keeping records of citizens because they are believed to associate with those who have a propensity to violence and crime and justify those kinds of interferences with that it 'serves public interests', that is a threat to democracy, whether intentional or not as it undermines several democratic principles. If such monitoring was to occur at a political gathering or protest, for example, the monitoring could have a chilling effect on freedom of association.[384] Even suspicionless surveillance unrelated to political views could have a chilling effect on free association and free speech, as the fear of having one's conversations monitored could lead to self-censoring.[385] For that reason, it should not be possible to justify interferences with privacy solely on the seriousness of the offence, as it makes it easier for politicians to override concerns about unjust privacy intrusions. Intentional suspicionless monitoring also raises questions about the rule of law. In addition to the issues discussed in chapter 6, which mostly had to do with foreseeability, suspicionless surveillance also raises questions about necessity and proportionality.

7.1.2 Is It Legitimate to Use Technology Preventively, Even If It Is Effective?

As mentioned in part 5.1.2, it is not enough for covert surveillance to pursue a legitimate aim to be justified. Apart from serving a legitimate objective, the surveillance must also *further* that objective to a certain degree. Thus, if the surveillance is unlikely to be effective, it should not be pursued. There are two aspects worth highlighting regarding the effectiveness of covert surveillance measures on crime reduction, especially concerning pre-emptive measures. The first aspect relates to the actual efficacy of surveillance measures, and the second relates to the justifications for using surveillance measures even if they are considered effective. While some studies suggest that electronic monitoring has a considerable effect on organised crime and terrorism, other studies show that they have a limited impact on crime reduction as criminal groups tend to adapt to the police's surveillance methods by changing the way they communicate and transport goods.[386]

[384] This was also the conclusion of the ECtHR in *Catt v. the United Kingdom*, §§ 123–128.
[385] See chapter 4.
[386] Compare Piza et al., 'CCTV Surveillance for Crime Prevention', 147–52; Slobogin and Brayne, 'Surveillance Technologies and Constitutional Law'; Cayford and Pieters, 'The Effectiveness of Surveillance Technology', 93–101. to Landau, *Surveillance or Security?*, chap. 5; Spapens, 'Interaction between Criminal Groups and Law Enforcement', 28–40; Nunn, 'Measuring Criminal Justice Technology Outputs'.

The differentiating and sometimes conflicting results can be explained by a lack of empirical data on many surveillance technologies, even when it comes to simple questions such as how many departments are using them or how they are deployed.[387] Another aspect of the effectiveness of covert surveillance is being able to understand the information it produces. As testified by Patrick Fitzgerald, who worked as a US attorney during many of the terrorism cases related to al Qaeda in the early 2000s, being privy to the plotting of a crime does not necessarily prevent its occurrence as it can be challenging to piece the information together:

> [P]eople talk cryptically, they harrumph, they refer to this guy, they refer to that guy, that place over there. It took us years to go back and look at those wiretaps […] with the benefit of witnesses, to figure out what was going on, know the hindsight and piece together what was being said.[388]

With that in mind, a finger of caution should be raised whenever governments justify the introduction of new surveillance techniques on the grounds of their effectiveness and 'ubiquity worldwide' in the absence of concrete evidence of their crime-reducing effect.[389] Even if it was concluded that surveillance measures dramatically reduce the number of crimes in society, the appropriateness of subjecting innocent people to surveillance could be questioned. While regulations such as the Patriot Act[390] probably result in more arrests and convictions than regulations that require probable cause for surveillance, the consequence of such laws is discrimination and social sorting.[391] This leads to the question of how proportionate mass surveillance and practices bordering on mass surveillance are.[392]

7.2 The ECtHR on the Balance of Public Security and Privacy

The idea of proportionality is one of the oldest principles of moral theory. When measuring the overall benefits of a proposed measure, leaders and individuals alike often weigh the costs of an action against what can be gained from it.[393] What distinguishes the principle of proportionality in the case law of the ECtHR from the proportionality principle in JWT is their

[387] See Slobogin and Brayne, 'Surveillance Technologies and Constitutional Law', 235.
[388] 9/11 Commission, 'National Commission on Terrorist Attacks Upon the United States Twelfth Public Hearing'.
[389] An example of this is the Swedish Government in SOU 2022:52, 119, 124, 169 and SOU 2022:19, 129, 204, 282–284.
[390] The Patriot Act was a US regulation that allowed for wiretapping of American citizens to obtain evidence of crime without having to prove probable cause. See footnote 122.
[391] See chapter 4.
[392] For example, proposals such as SOU 2022:19 and SOU 2022:52.
[393] See Bellaby, 'Intelligence and the Just War Tradition', 15.

approach to privacy harms. To tie back to chapter 6, JWT requires reliable information that a serious crime involving a particular danger to society will take place for it to condone intentional surveillance of innocents, while the ECtHR seems to accept such intrusions provided that the offence is sufficiently serious and the intrusion is not manifestly unfounded. That is, as long as the public good outweighs the harm to the individual caused by the intrusion. This indicates that JWT attaches greater importance to the damage caused by privacy intrusions than Article 8 ECHR, as it recognizes "that not only harms but also harmless wrongs should count on the cost side of the proportionality […] equation in the context of surveillance."[394]

7.2.1 Harm-based Approach to Proportionality vs Need-Based Approach to Proportionality

The advantage of a harm-based approach to proportionality is that it recognizes that privacy harms consist of more than actual damage to individuals in the form of 'loss of control over personal information' that can affect a person's personal esteem in the eyes of others or their opportunities to find work because of the stigma of being associated as a criminal.[395] As will be developed in section 7.3, a loss of privacy can also result in autonomy harm, which involves "restricting, undermining, inhibiting, or unduly influencing people's choices" [396] in ways that undermine democratic participation. The harm based-approach to proportionality in JWT also corresponds better to the principle of necessity than the ECtHR's need-based approach, as it ensures that no more intrusive measures than necessary are used to neutralise a threat to public security. Therefore, liability should be at the centre of the discussion when discussing proportionality in relation to covert surveillance practices.

For covert surveillance of non-liable individuals to be justified, the threat to the public to be prevented must be significantly much more damaging than the harm to the individual caused by the surveillance. There is a reason why intelligence agencies often have more intrusive surveillance measures available to them than law-enforcement agencies, and that is because they respond to different types of threats. Responding to threats that disrupt the public order is not the same as responding to threats that disrupt critical societal functions and threaten the state's existence. Since threats that threaten the state's existence would impact everybody's individual rights and not only the target of the surveillance, suspicionless surveillance is more

[394] Rønn and Lippert-Rasmussen, 'Out of Proportion?', 2.
[395] See Solove and Citron, 'Privacy Harms', 39, 55.
[396] Solove and Citron, 45.

justified when it comes to national security threats. Law- enforcement agencies should therefore not have access to the same technological means when fighting less serious crimes such as the ones described in the Swedish draft proposal in chapters 3 and 5. When investigating those types of crimes, the person's liability should be the decisive factor when deciding whether to subject a person to surveillance.

7.2.2 The Difference Between Posing a Threat to Society and Facilitating a Threat to Society

Having discussed why liability should play a part in the proportionality assessment, this section will discuss how liability could be used to assess the legitimacy of subjecting someone to covert surveillance. Out of all the suggested ways of viewing proportionality presented in this essay, Rønn and Lippert-Rasmussen's modified version of proportionality under JWT is the most preferable. This is because the author's distinction between narrow and wide proportionality provides the most nuanced approach to the connection between liability and targeting. By distinguishing between intentional and unintentional intrusions upon liable and non-liable individuals, it becomes clearer in which cases the target for surveillance has made himself accountable for a threat in such a way that the harm of the surveillance can be justified.[397] This is because liability helps to distinguish between just and unjust privacy intrusions; unjust privacy intrusions in this case defined as 'surveillance operations directed towards individuals that are unlikely to contribute with information of value to a criminal investigation because of their detachment from the crime under investigation.' While it is beyond the scope of this essay to decide on the appropriate amount of 'threat contribution' necessary to become liable for defensive harms, it should take more than just associating with a known or believed criminal or crime scene to become liable for covert surveillance. For example, participation in a political group that has made statements that can be interpreted as a threat of violence or the existence of a call log that shows that a person not currently under criminal suspicion has interacted with a key suspect in close proximity to the crime under investigation.[398]

Another critical aspect of the wide proportionality assessment that Rønn and Lippert-Rasmussen have not really highlighted is how the intrusiveness of the surveillance should factor into the operation's legitimacy. If covert surveillance is the only way forward in an investigation

[397] This is, of course, assuming that the threat can be classified as an unjust threat to public security, as covert surveillance should never be undertaken unless there is an actual threat to public safety.
[398] This first example is inspired by a similar argument made by Nathan in, 'Liability to Deception and Manipulation', 377.

of a serious threat to the public, the choice to use a less invasive means of surveillance can make up for the lack of individualised suspicion until more information about the person's involvement in the threat is known. For that reason, it might be a good idea for legislation on covert surveillance to place obstacles in the way of accessing sensitive data until the police can demonstrate its necessity for the investigation. Such uncertainty in terms of liability should also result in stricter rules for data processing, as suspicionless surveillance is more likely to result in irrelevant information to the investigation. For example, a prohibition of retaining personal data of no further use to the investigation beyond a specified period of time.

7.3 The ECtHR and Autonomy

Now that the more 'legal' aspects of restricting the right to privacy have been discussed, it is time to address the issue from an autonomy perspective, as that is one of the sub-purposes of this essay.[399] A recurring question in the Court's case law is if the privacy intrusion caused by covert surveillance can be 'justified in a democratic society.' The right to privacy in Article 8 ECHR protects several essential features in a democracy, explicitly and by its mere existence. The values of privacy for democracy that the Court has explicitly acknowledged include democratic self-governance[400], informational self-determination[401] and freedom of expression[402], which can be seen as different expressions of autonomy. Despite recognizing that autonomy is essential for democracy, it is unusual that the interest of autonomy plays a decisive role in the 'democratic necessity test.' If the Court concludes that a government has failed to strike a fair balance between the interests of privacy and public security, it is often for procedural reasons because the regulation has failed to provide "sufficiently precise, effective and comprehensive [*safeguards*] on the ordering, execution and potential redressing of such measures."[403]

7.3.1 Societal Considerations vs Individualistic Considerations

Much like the classical debate on privacy and security,[404] the individual consequences caused by privacy intrusions have been given more attention than the collective consequences of such

[399] See research question 3 in part 1.1.
[400] See *Catt v. the United Kingdom*, § 124.
[401] See *Breyer v. Germany*, § 75.
[402] *Big Brother Watch v. the United Kingdom*, §§ 450–458.
[403] *Szabó and Vissy v. Hungary*, § 89. Also see chapter 5.
[404] See part 4.2.2.

intrusions in the jurisprudence of the ECtHR,[405] which is unfortunate. As argued elsewhere in this thesis, the inhibiting effects of legislation on covert surveillance deserve more attention, considering its potential impact on democratic participation, which can be collaborated by various human rights organisations. Reports from INCLO, for example, indicate that surveillance technologies have been used to spy on activists, journalists and others expressing opinions not supported by the government, ultimately resulting in 'warning conversations', unlawful searches and blocking of online content.[406]

7.3.2 A Comparison Between 'Public Interest' in Article 8 and Article 10 ECHR

One possible way to enhance the collective importance of privacy could be to draw inspiration from the ECtHR's approach to 'democratic necessity' in freedom of expression cases. In contrast to privacy cases, where the margin of appreciation is framed in rather generous terms, the margin of appreciation in Article 10 cases is much more limited. For Article 10 ECHR to be restricted, it must be justified by an 'overriding public interests', which includes an assessment of the potential impact of the restrictive measures on the applicant's exercise of political rights.[407] If the Court had a similar approach to privacy and attached greater importance to the democratic consequences of covert surveillance, perhaps the risk of self-censorship would not be as significant, as greater evidence of necessity would be required to initiate surveillance practices.

7.4 Ambiguities in ECtHR Case Law – is the Margin of Appreciation the Problem?

In nearly every examination of surveillance cases, the ECtHR underscores its subsidiary role to national courts and authorities,[408] as is both expected and required of them since it is not the

[405] An example of this is *Weber v. Saravia v. Germany* which concerned the potential chilling effects on freedom of expression caused by bulk interception. Since the law was considered to have adequate and effective procedural safeguards against surveillance abuse, the potential impact of the legislation of journalistic freedom and free speech in general was not considered to be serious enough to give rise to a violation. See paragraphs 147–153.

[406] See INCLO, 'Surveillance and Democracy: Chilling Tales from Around the World'; INCLO, 'Spying on Dissent Surveillance Technologies and Protest'. Also see Penney, 'Chilling Effects', 147–73. The study explored how traffic to Wikipedia articles on topics that raise privacy concerns for Wikipedia users changed after the Snowden revelations in 2013. It found that there was a decline in page views on articles related to terrorism and other subjects associated with government surveillance.

[407] *Weber v. Saravia v. Germany*, § 149. Also see *Sunday times v. the United Kingdom*, §§ 59–61; *Stoll v. Switzerland*, §§ 101–102; *Pentikäinen v. Finland*, §§ 95–101.

[408] See e.g., *Klass v. Germany*, § 49; *Leander v. Sweden*, §§ 58-59; *Kvasnica v. Slovakia*, § 80; *Kennedy v. the United Kingdom*, § 154; *Weber and Saravia*, § 106; *Breyer v. Germany*, § 79; *Big Brother Watch v. the United Kingdom*, § 274; *Szabó and Vissy v. Hungary*, § 57; *Roman Zakharov v. Russia*, § 232; *Dragojević v. Croatia*, § 84.

role of international courts to exercise functions traditionally performed by the state. Judicial review of the acts of national governments by supranational courts therefore raises questions about democratic legitimacy, as such 'law-making' or 'judicial veto' undermines publicly deliberated decisions adapted to local conditions.[409] The ECtHR is therefore correct to point out that "it is not for [*it*] to substitute its own assessment of the merits of the contested measure […] for that of the competent national authorities"[410] as they are in a "better position to obtain and assess local knowledge which the Court may either not have or the significance of which it may misjudge."[411] This becomes even more evident in national and public security matters. Since the ECtHR does not have access to the information necessary to make an informed decision regarding public safety, those charged with upholding public security (i.e., the nation-states) must be allowed to adopt national policy on these matters relatively undisturbed. Autonomous decision-making is therefore essential to the well-being of the state and society, but then again, so is protecting human rights.

The reason why the right to privacy and other international human rights were created in the first place was to protect individuals from arbitrary exercise of state power.[412] To provide such supranational oversight, the ECtHR must be allowed to put pressure on the Convention States and demand that they act according to their Convention commitments. This, in turn, requires that the ECtHR is vocal about how Convention rights should be interpreted, which is not always the case for politically sensitive topics such as public security. The State's margin of appreciation in Article 8 cases concerning covert surveillance therefore needs to be adjusted so that the ECtHR can ensure that the Huvig/Weber criteria and the principle of proportionality are realised to a greater extent.

7.4.1 Why Does the ECtHR Leave Certain Questions Open for Interpretation?

Since it can be established that the margin of appreciation is partly to blame for the ambiguities in the ECtHR's case law concerning covert surveillance, the natural question becomes why. Why does the Court avoid questions such as the necessary degree of criminal suspicion for covert surveillance when it is evident from its case law that those questions are crucial to

[409] See von Staden, 'The Democratic Legitimacy of Judicial Review beyond the State', 1023–26; De Brabandere, 'The Impact of Supranationalism on State Sovereignty from the Perspective of the Legitimacy of International Organisations', 1–2.
[410] *McDonald v. the United Kingdom*, § 57.
[411] Greer, *The Exceptions to Articles 8 to 11 of the European Convention on Human Rights*, 33.
[412] See part 2.1.1.

assessing the legitimacy of covert surveillance measures?[413] One theory, which holds appeal, is that the Court is exercising restraint for political reasons. As established in the section above, supranational courts have an inherent democratic deficit as they are not popularly elected. That, combined with the Court relying on the Convention States for judicial enforcement, has made it reluctant to aggravate the signatories, as the practical impact of the Court's judgements largely depends upon the goodwill of the Convention States. Since the Court's legitimacy relies on the Convention state's support, it is essential for the Court that compliance with the Convention is a status marker so that non-compliance is discouraged by other Convention States and generates political pressure to comply with the Court's decisions. By choosing to defer politically controversial issues such as same-sex marriage, euthanasia and security issues to the Convention States, the Court is establishing credibility and building leverage to advance questions of particular importance to the Court in the future.[414] While it is understandable that the Court is using the margin of appreciation as a strategic tool to achieve long-term democratic goals, it is also problematic as it leaves the Convention rights up for interpretation.

7.4.2 Is There Anything That Can Be Done to Strengthen the Role of The Court?

As demonstrated in the section above, the risk of national non-compliance is the Achilles heel of the right to privacy under ECHR. If the ECHR had more robust enforcement mechanisms, the Court would probably be more inclined to challenge the reasons given by the Convention States for introducing new surveillance measures as it would be less dependent on its reputation for the execution of judgements. Therefore, it would be worth investigating how the enforcement mechanisms of the ECHR could be strengthened. Since the EU has an economic sanctioning system, it might be possible to draw inspiration from there.[415] However, since the EU and the Council of Europe have slightly different functions,[416] it should not be assumed that the same approach would be applicable here. Therefore, more research on this area is necessary

[413] Otherwise, it would make no sense for the Court to emphasise the importance of limiting the categories of people to be monitored, the nature of offences that can give rise to surveillance, the duration of surveillance measures etc. over and over again in the Huvig/Weber criteria.
[414] See Zarbiyev, 'Judicial Activism in International Law--A Conceptual Framework for Analysis', 276–78; Dothan, 'Judicial Tactics in the European Court of Human Rights'.
[415] The rule of law framework mentioned can be found in Article 2 TEU and Article 7 TEU.
[416] While the Council of Europe and the EU share and aim to uphold the same fundamental values – respect for human rights, democracy and the rule of law - they are separate entities with different roles. Besides its role as a protector of human rights, the EU is also a political and economic entity that acts as a unified front in the global market. Compare Article 1 of The Statute of the Council of Europe to Article 3 TEU. Also see Joris and Vandenberghe, 'The Council of Europe and the European Union'.

to find a suitable enforcement model adapted to the needs of the ECtHR and the Convention States.

Something else that could strengthen the role of the ECtHR as a human rights adjudicator is a greater understanding of the Court's role in a democracy. That supranational courts like the ECtHR do not have the same democratic legitimacy as national governments and parliaments is not a disputed fact. From a democratic point of view, however, this might not be as problematic as it seems. Since respect for the rule of law includes respect for human rights, there is an element of protection against the 'will of the majority' in modern democracies.[417] As observed by Benvenisti, whenever minorities exist, democracy is prone to undermine their interests by monopolising political power and using it to further their own interest instead of protecting legally recognized religious, national and racial minority rights.[418] Since privacy could be regarded as a minority interest when set against the universally recognized interest in public security, the ECtHR could be said to uphold the democratic balance of power when adjudicating privacy cases. Another crucial point to remember when it comes to democratic legitimacy and national sovereignty is that the Convention States have consented to be bound by the Convention, which includes a commitment to respect and uphold the ECtHR's interpretation of the rights therein.[419] It is therefore a weak argument to use national sovereignty as an excuse for not having to comply with the Convention, as it was a choice made by democratically elected representatives to join the Convention in the first place.

[417] See chapter 4 which describes the elements that can be attributed to the 'thick' version of the rule of law.
[418] See Benvenisti, 'MARGIN OF APPRECIATION, CONSENSUS, AND UNIVERSAL STANDARDS', 849–50.
[419] See Article 1 ECHR; Article 19 ECHR; Article 32 ECHR.

8 Conclusion

After examining the current security trends in domestic and foreign surveillance laws, the findings of this study suggest that the European framework concerning covert surveillance is inadequate in some parts when it comes to protection against arbitrary interference with privacy. This is not to say that the Court has been or is incapable of upholding the democratic values associated with and made possible by the right to privacy, but rather that this role could be enhanced with some changes to its current jurisprudence. Right now, the Court's notion of privacy is too individualistic and concerned with preventing 'measurable damage' from privacy intrusions rather than protecting individuals from state interference in general. Suppose the ECtHR was to look at privacy more as a collective right as it does with Article 10 ECHR. If so, this could perhaps be amended as the societal value of privacy would be given more significance. However, this presupposes that the view of privacy has given rise to the ambiguities in the Court's case law and not the fear of overstepping politically. Regardless of which, the consequence of the ambiguities in the Court's case law is that Convention states are left to guess which standard of privacy applies in different situations, which could undermine the general level of privacy protection in Europe. For that reason, the ECtHR needs to be more detailed in its rulings as that would make it harder for Convention states to invoke public security as an exception to privacy excessively or for purposes other than those set out in the Article 8 ECHR. Because, after all, how can the Court expect Convention states to uphold a certain standard of privacy if it is unknown?

8.1 The Importance of Societal Debate

The Hungarian and Polish experience demonstrates how fragile democracies are and how quickly democratic principles, such as the rule of law, can be set aside without proper safeguards in place and an awareness of the importance of 'bureaucratic obstacles' standing in the way of in this case: "interference with the lawyer-client privilege"[420], "oversight of […] metadata collection"[421], and "judicial independence and […] impartiality."[422]

[420] Venice Commission, *Opinion on the Act of 15 January 2016 amending the Police Act and certain other Acts, adopted by the Venice Commission at its 107th Plenary Session (Venice, 10-11 June 2016)*, § 79
[421] Venice Commission, *Opinion on the Act of 15 January 2016 amending the Police Act and certain other Acts, adopted by the Venice Commission at its 107th Plenary Session (Venice, 10-11 June 2016)*, § 123
[422] Venice Commission, *Urgent Joint Opinion of the Venice Commission and the Directorate General of Human Rights and Rule of Law (DGI) of the Council of Europe on amendments to the Law on the Common courts*, *the Law on the Supreme court and some other Laws, issued pursuant to Article 14a of the Venice Commission's Rules of Procedure on 16 January 2020*, *endorsed by the Venice Commission on 18 June by a written procedure replacing the 123rd Plenary Session*, § 24

If Sweden chooses to go down the path of proactive policing, the new surveillance measures not only risk conflicting with the ECHR and the right to privacy. In addition, there is a risk that the framework could make it easier for an authoritarian regime to exercise arbitrary control over citizens by spying on dissidents and creating an atmosphere of distrust that impedes democratic interaction, as the framework requires fewer substantial arguments for initiating surveillance. Therefore, before any policy changes are made, it would be wise to consider the long-term effects of the legislative proposals on democracy - and not only the anticipated short-term gains in the fight against criminal networks. After all, there is little point in the state trying to create a society free from crime and threats to public security if the overall cost is severe loss of personal freedom and facilitation of authoritarian tendencies. When reflecting on how covert surveillance can be kept within the limits of democratic values and principles, some of the questions policy-makers could ask themselves are:

1. **Why is there a need to introduce new surveillance measures?** What identified problems does the proposal seeks to address, and what suggests that the proposed measures would be better or more efficient in overcoming those problems?

2. **How big is the 'danger' that the technology will allegedly reduce, and how does it compare to the damage caused by the surveillance?**[423] Are the risks associated with not enacting the proposal proportional to the expected loss of privacy that the proposal would entail?

3. **What risks to social cohesion and public deliberation does the proposal entail?** Is there a risk that enacting the proposal could result in unintended consequences, such as self-censorship, racial profiling or other types of discrimination, and in that case, what legal safeguards are in place to prevent such abuses?

4. **Does the proposed regulation differentiate between liable and non-liable targets of surveillance to a satisfactory degree?** Are there different standards of proportionality depending on the target's actual risk to society, and how is it reflected in the proposed legislation? For example, are there obstacles in the way of subjecting suspects of minor

[423] A similar argument has been put forward by Stanley in , 'Six Questions to Ask Before Accepting a Surveillance Technology'.

crimes and innocents to surveillance measures capable of collecting more than just peripheral data?

5. **For preventive surveillance: Who is the real beneficiary of the covert investigation? The police or the public?** If the answer is the police, this indicates that the surveillance might be undertaken for the wrong reasons, as suspicionless surveillance should only be used to prevent an even bigger threat to the public and not to facilitate police work in general.

…

When the European privacy framework is not as strong as it could be, it becomes increasingly important that discussions such as these take place at a national level since there is no guarantee that a government with totalitarian predispositions would respect the Court's judgements. In view of this, European states must try to resist the temptation to introduce more intrusive surveillance measures unless absolutely necessary, as it is usually too late to reinforce the protection of privacy when it has already been lost.

8.2 Final Remarks

The state's duty of keeping the citizenry safe is and should always be a governmental priority. That does not mean that interest in privacy should have to give way to the interest of security at all times or that both interests cannot be accommodated at the same time. While a perfect balance between privacy and public security is probably not achievable, JWT and just surveillance principles show that there is a way, at least theoretically, to conduct surveillance in a way that safeguards moral and legal norms while responding to pressing security needs. Technologically, we are already living in the Orwellian society of 1984. If the police had the necessary authorisation, they could have eyes and ears *everywhere* since there are endless ways to manipulate technological devices, and almost everyone has a smartphone, computer or tablet at arm's reach. Whether the technology will be used to exercise control over citizens or to secure a safe space to exercise fundamental freedoms depends on how these issues are debated in national parliaments, intergovernmental organisations and interpreters of international law and the substantial safeguards against surveillance abuse resulting from those conversations. If collective action is taken now, it is not too late to stop Big Brother from becoming a worldwide phenomenon. If not, it is not a question of if but when Orwell's dystopian prophesies will be realized to some extent.

Bibliography

Official Swedish Publications

Government Bills (Prop.)

Prop. 1975/76:202 Med förslag till nya regler om telefonavlyssning vid förundersökning m.m.

Prop.1988/89:124 Om vissa tvångsmedelsfrågor.

Prop. 1993/94:117 Inkorporering av Europakonventionen och andra fri- och rättighetsfrågor

Prop. 1995/96:85 Hemlig kameraövervakning.

Prop. 2002/03:74 Hemliga tvångsmedel - offentliga ombud och en mer ändamålsenlig reglering.

Prop. 2005/06:178 Hemlig rumsavlyssning.

Prop. 2009/10:80 En reformerad grundlag.

Prop. 2011/12:55 De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation.

Prop. 2013/14:237 Hemliga tvångsmedel mot allvarliga brott.

Prop. 2019/20:64 Hemlig dataavläsning.

Swedish Government Official Reports (SOU Series)

SOU 1968:4 Handläggningen av säkerhetsfrågor.

SOU 1975:95 Telefonavlyssning.

SOU 1995:47 Tvångsmedel enligt 27 och 28 kap. RB samt polislagen: slutbetänkande

SOU 1998:46 Om buggning och andra hemliga tvångsmedel.

SOU 2009:1 En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen.

SOU 2012:44 Hemliga tvångsmedel mot allvarliga brott.

SOU 2022:19 Utökade möjligheter att använda hemliga tvångsmedel.

SOU 2022:50 Bättre möjligheter att verkställa frihetsberövanden.

SOU 2022:52 Utökade möjligheter att använda preventiva tvångsmedel.

Ministry Publications (Ds Series)

Ds Ju 1981:22 Hemlig avlyssning m.m.

Ds 2005:21 Tvångsmedel för att förebygga eller förhindra allvarlig brottslighet.

Terms of Reference of a Commission of Inquiry

Kommittédirektiv 2020:104 Utökade möjligheter att använda hemliga tvångsmedel.

Kommittédirektiv 2021:102 Preventiva tvångsmedel för att förhindra allvarlig brottslighet.

Kommittédirektiv 2021:113 Tilläggsdirektiv till utredningen Preventiva tvångsmedel för att förhindra allvarlig brottslighet.

Kommittédirektiv 2022:13 Tilläggsdirektiv till Utredningen om utökade möjligheter att använda hemliga tvångsmedel.

Kommittédirektiv 2022:32 Tilläggsdirektiv till Utredningen om preventiva tvångsmedel.

Kommittédirektiv 2022:104 Tilläggsdirektiv till Utredningen om preventiva tvångsmedel.

Official European Publications

EU Preparatory Works

Communication of 30 August 2006 from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, *Governance in the European Consensus on Development Towards a harmonised approach within the European Union*, COM (2006) 421 final.

Official Journal of the European Union (OJEU). 14.12.2007, No C 303. [s.l.]. ISSN 1725-2423. "Explanations relating to the Charter of Fundamental Rights."

Article 29 Data Protection Working Party, *Opinion 01/13 providing further input into the discussion of the Draft Police and Criminal Justice Data Protection Directive,* 00379/13/EN WP 201, 26 February 2013.

Communication of 11 March 2014 from the Commission to the European Parliament and the Council, *A new EU Framework to strengthen the Rule of Law*, COM/2014/0158 final.

Other Official Publications

The Parliament of the Commonwealth of Australia and House of Representatives, *Explanatory Memorandum of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*, 2019-2020.

Case Law

Judgements from the European Court of Justice

Judgement of 21 December 2016, *Post-och telestyrelsen, and Secretary of State for the Home Department v Tom Watson, Peter Brice and Geoffrey Lewis*, joined cases C-203/15 and C-698/15, EU: C:2016:970.

Judgement of 2 March 2021, *H.K. v. Prokuratuur*, C-746/18, EU:C:2021:152.

Judgements From the European Court of Human Rights

Handyside v. the United Kingdom, 7 December 1976, Series A no. 24.

Ireland v. the United Kingdom, 18 January 1978, Series A no. 25.

Tyrer v. the United Kingdom, 25 April 1978, Series A no. 26.

Klass and Others v. Germany, 6 September 1978, Series A no. 28.

The Sunday Times v. the United Kingdom (no. 1), 26 April 1979, Series A no. 30.

Malone v. the United Kingdom, 2 August 1984, Series A no. 82.

M v. France, no. 10078/82, Decision of 13 December 1984 (Plenary, admissibility).

Leander v. Sweden, 26 March 1987, Series A no. 116.

Kruslin v. France, 24 April 1990, Series A no. 176-A.

Huvig v. France, 24 April 1990, Series A no. 176-B.

Kopp v. Switzerland, 25 March 1998, Reports of Judgments and Decisions 1998-II.

Lambert v. France, 24 August 1998, Reports of Judgments and Decisions 1998-V.

Valenzuela Contreras v. Spain, 30 July 1998, Reports of Judgments and Decisions 1998-V.

Osman v. the United Kingdom, 28 October 1998, Reports of Judgments and Decisions 1998 VIII.

P.G. and J.H. v. the United Kingdom, no. 44787/98, ECHR 2001-IX.

Greuter v. the Netherlands (dec.), no. 40045/98, 19 March 2002.

Pretty v. the United Kingdom, no. 2346/02, ECHR 2002-III.

Christine Goodwin v. the United Kingdom [GC], no. 28957/95, ECHR 2002-VI.

Stec and Others v. the United Kingdom (dec.) [GC], nos. 65731/01 and 65900/01, ECHR 2005-X.

Vetter v. France, no. 59842/00, 31 May 2005.

Segerstedt-Wiberg and Others v. Sweden, no. 62332/00, ECHR 2006-VII.

Weber and Saravia v. Germany (dec.), no. 54934/00, ECHR 2006-XI.

Coban v. Spain (dec.), no. 17060/02, 25 September 2006.

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, no. 62540/00, 28 June 2007.

Folgerø and Others v. Norway [GC], no. 15472/02, ECHR 2007-III.

Stoll v. Switzerland [GC], no. 69698/01, ECHR 2007-V.

S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, ECHR 2008.

Iordachi and Others v. Moldova, no. 25198/02, 10 February 2009.

Bykov v. Russia [GC], no. 4378/02, 10 March 2009.

Kvasnica v. Slovakia, no. 72094/01, 9 June 2009.

Uzun v. Germany, no. 35623/05, ECHR 2010 (extracts).

Kennedy v. the United Kingdom, no. 26839/05, 18 May 2010.

El-Masri v. the former Yugoslav Republic of Macedonia [GC], no. 39630/09, ECHR 2012.

Michaud v. France, no. 12323/11, ECHR 2012.

Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands, no. 39315/06, 22 November 2012.

M.K. v. France, no. 19522/09, 18 April 2013.

Peruzzo and Martens v. Germany, nos. 7841/08 and 57900/12, 4 June 2013.

McDonald v. the United Kingdom, no. 4241/12, 20 May 2014.

Dragojević v. Croatia, no. 68955/11, 15 January 2015.

Roman Zakharov v. Russia [GC], no. 47143/06, ECHR 2015.

Pentikäinen v. Finland [GC], no. 11882/10, ECHR 2015.

R.E. v. the United Kingdom, no. 62498/11, 27 October 2015.

Szabó and Vissy v. Hungary, no. 37138/14, 12 January 2016.

Karabeyoğlu v. Turkey, no. 30083/10, 7 June 2016.

Magyar Helsinki Bizottság v. Hungary [GC], no. 18030/11, 8 November 2016.

A.H. and Others v. Russia, nos. 6033/13 and 15 others, 17 January 2017.

İrfan Güzel v. Turkey, no. 35285/08, 7 February 2017.

Mustafa Sezgin Tanrıkulu v. Turkey, no. 27473/06, 18 July 2017.

Bărbulescu v. Romania [GC], no. 61496/08, 5 September 2017.

Dudchenko v. Russia, no. 37717/05, 7 November 2017.

Ben Faiza v. France, no. 31446/12, 8 February 2018.

Libert v. France, no. 588/13, 22 February 2018.

Benedik v. Slovenia, no. 62357/14, 24 April 2018.

Khadija Ismayilova v. Azerbaijan, nos. 65286/13 and 57270/14, 10 January 2019.

Catt v. the United Kingdom, no. 43514/15, 24 January 2019.

Bosak and Others v. Croatia, nos. 40429/14 and 3 others, 6 June 2019.
Breyer v. Germany, no. 50001/12, 30 January 2020.
Gaughran v. the United Kingdom, no. 45245/15, 13 February 2020.
P.N. v. Germany, no. 74440/17, 11 June 2020.
Privacy International and Others v. the United Kingdom, no. 46259/16, 4 September 2020.
Big Brother Watch and Others v. the United Kingdom [GC], nos. 58170/13 and 2 others, 25 May 2021.
Centrum för rättvisa v. Sweden [GC], no. 35252/08, 25 May 2021.
Zoltán Varga v. Slovakia, nos. 58361/12 and 2 others, 20 July 2021.
Azer Ahmadov v. Azerbaijan, no. 3409/10, 22 July 2021.
Vasil Vasilev v. Bulgaria, no. 7610/15, 16 November 2021.
Ekimdzhiev and Others v. Bulgaria, no. 70078/12, 11 January 2022.
Adomaitis v. Lithuania, no. 14833/18, 18 January 2022.
Deveci v. Türkiye (dec.), no. 42785/11, 28 June 2022.

European Commission Decisions

Esbester v. the United Kingdom, no 18601/91, Commission decision of 2 April 1993, Decisions and Reports 78-A.

Literature

Adler, E. Scott, and Thad E. Hall. 'Ballots, Transparency, and Democracy'. *Election Law Journal: Rules, Politics, and Policy* 12, no. 2 (June 2013): 146–61. https://doi.org/10.1089/elj.2012.0179.

Ahmed, Shamila. 'Citizenship, Belonging and Attachment in the "War on Terror"'. *Critical Criminology* 24, no. 1 (March 2016): 111–25. https://doi.org/10.1007/s10612-015-9279-2.

Akdogan, Mizgin. 'Överskottsinformation från hemliga tvångsmedel – En analys av hur regleringen av överskottsinformation från hemliga tvångsmedel bör utformas, med särskilt beaktande av SOU 2018:61'. *Juridisk Publikation*, no. 2/2019 (n.d.): 399–417.

Ali, Asghar, Nazim Rahim, and Syed Mussawar Hussain Bukhari. 'The Just War Theory and Human Rights Violations: What Does International Law Tell?' *Global Legal Studies Review* IV, no. I (30 December 2019): 1–6. https://doi.org/10.31703/glsr.2019(IV-I).01.

Aquilina, Kevin. 'Public Security versus Privacy in Technology Law: A Balancing Act?' *Computer Law & Security Review* 26, no. 2 (March 2010): 130–43. https://doi.org/10.1016/j.clsr.2010.01.002.

Arroyo Moliner, Liliana, and Philippe M. Frowd. 'Social Sorting'. In *The SAGE Encyclopedia of Surveillance, Security, and Privacy*, edited by Bruce A. Arrigo. SAGE Publications, 15 June 2016.

Ashworth, Andrew, Lucia Zedner, and Patrick Tomlin, eds. *Prevention and the Limits of the Criminal Law*. Oxford University Press, 2013. https://doi.org/10.1093/acprof:oso/9780199656769.001.0001.

Bachmaier Winter, Lorena. 'Proportionality, Mass Surveillance and Criminal Investigation: The Strasbourg Court Facing Big Brother'. In *Proportionality in Crime Control and Criminal Justice*, edited by Emmanouil Billis, Nandor Knust, and Jon Petter Rui. Hart Publishing, 2021. https://doi.org/10.5040/9781509938636.

Bailey, John, and Lucía Dammert, eds. *Public Security and Police Reform in the Americas*. Pittsburgh: University of Pittsburgh Press, 2006.

Beckman, Ludvig. 'Godtagbart i ett demokratiskt samhälle? De hemliga tvångsmedlen och rätten till personlig integritet. | SvJT'. *Svensk Juristtidning*, no. 1 (2006): 1–22.

Bellaby, Ross. 'Intelligence and the Just War Tradition'. In *National Security Intelligence and Ethics*, by Seumas Miller, Mitt Regan, and Patrick F. Walsh, 7–20, 1st ed. London: Routledge, 2021. https://doi.org/10.4324/9781003164197-3.

Bellaby, Ross. ‘What’s the Harm? The Ethics of Intelligence Collection’. *Intelligence and National Security* 27, no. 1 (February 2012): 93–117. https://doi.org/10.1080/02684527.2012.621600.

Bellaby, Ross. ‘Justifying Cyber-Intelligence?’ *Journal of Military Ethics* 15, no. 4 (1 October 2016): 299–319. https://doi.org/10.1080/15027570.2017.1284463.

Bellaby, Ross. ‘Too Many Secrets? When Should the Intelligence Community Be Allowed to Keep Secrets?’ *Polity* 51, no. 1 (January 2019): 62–94. https://doi.org/10.1086/701165.

Benvenisti, Eyal. ‘MARGIN OF APPRECIATION, CONSENSUS, AND UNIVERSAL STANDARDS’. *Margin of Appreciation, Consensus and Universal Standards*, 1 January 1999.

Bernal, Paul. ‘Data Gathering, Surveillance and Human Rights: Recasting the Debate’. *Journal of Cyber Policy* 1, no. 2 (2 July 2016): 243–64. https://doi.org/10.1080/23738871.2016.1228990.

Besser-Jones, Lorraine. ‘Just War Theory, Legitimate Authority, and the “War” on Terror’. In *Philosophy 9/11: Thinking About the War on Terrorism*, edited by Timothy Shanahan. Open Court, 2005.

Biletzki, Anat. *Philosophy of Human Rights: A Systematic Introduction*. Routledge, 2019.

Bislev, Sven. ‘Globalization, State Transformation, and Public Security’. *International Political Science Review* 25, no. 3 (July 2004): 281–96. https://doi.org/10.1177/0192512104043017.

Björklund, Fredrika. ‘Pure Flour in Your Bag: Governmental Rationalities of Camera Surveillance in Sweden’. *Information Polity* 16, no. 4 (24 December 2011): 355–68. https://doi.org/10.3233/IP-2011-0260.

Boehme-Neßler, Volker. ‘Privacy: A Matter of Democracy. Why Democracy Needs Privacy and Data Protection’. *International Data Privacy Law* 6, no. 3 (August 2016): 222–29. https://doi.org/10.1093/idpl/ipw007.

Born, H., and Marina Caparini, eds. *Democratic Control of Intelligence Services: Containing Rogue Elephants*. Aldershot, England; Burlington, VT: Ashgate, 2007.

Bowling, Ben, and Coretta Phillips. ‘Disproportionate and Discriminatory: Reviewing the Evidence on Police Stop and Search’. *Modern Law Review* 70, no. 6 (2007): 936–61. https://doi.org/10.1111/j.1468-2230.2007.00671.x.

Brown, Ian, and Douwe Korff. ‘Terrorism and the Proportionality of Internet Surveillance’. *European Journal of Criminology* 6, no. 2 (March 2009): 119–34. https://doi.org/10.1177/1477370808100541.

Bruce, Ingvild. 'The Preventive Use of Surveillance Measures for the Protection of National Security - a Normative and Comparative Study of Dutch, Norwegian and Swedish Law', 2020.

Burnay, Matthieu. *Chinese Perspectives on the International Rule of Law: Law and Politics in the One-Party State*. Leuven Global Governance. Cheltenham, UK Northampton, MA, USA: Edward Elgar Publishing, 2018.

Buzan, Barry. 'Rethinking Security after the Cold War'. *Cooperation and Conflict* 32, no. 1 (March 1997): 5–28. https://doi.org/10.1177/0010836797032001001.

Cameron, Iain. *National Security and the European Convention on Human Rights*. Brill | Nijhoff, 2000. https://doi.org/10.1163/9789004480902.

Cameron, Iain. 'The Influence of 9/11 on Swedish Anti-Terrorism Policy and Measures'. In *The Long Decade*, edited by David Jenkins, Amanda Jacobsen, and Anders Henriksen, 209–26. Oxford University Press, 2014. https://doi.org/10.1093/acprof:oso/9780199368327.003.0012.

Campos, Andre Santos, and José Gomes André, eds. *Challenges to Democratic Participation: Antipolitics, Deliberative Democracy, and Pluralism*. Lanham, Maryland: Lexington Books, 2014.

Carothers, Thomas, and Benjamin Press. *Understanding and Responding to Global Democratic Backsliding*. Washington, D.C.: Carnegie Endowment for International Peace, 2022. https://carnegieendowment.org/2022/10/20/understanding-and-responding-to-global-democratic-backsliding-pub-88173.

Carpenter, Christine. 'Privacy and Proportionality: Examining Mass Electronic Surveillance under Article 8 and the Fourth Amendment'. *International and Comparative Law Review* 20, no. 1 (1 June 2020): 27–57. https://doi.org/10.2478/iclr-2020-0002.

Cavelty, Myriam Dunn, and Matthias Leese. 'Politicising Security at the Boundaries: Privacy in Surveillance and Cybersecurity'. *European Review of International Studies* 5, no. 3 (17 December 2018): 49–69. https://doi.org/10.3224/eris.v5i3.03.

Cayford, Michelle, and Wolter Pieters. 'The Effectiveness of Surveillance Technology: What Intelligence Officials Are Saying'. *The Information Society* 34, no. 2 (15 March 2018): 88–103. https://doi.org/10.1080/01972243.2017.1414721.

Choo, Kim-Kwang Raymond, and Rick Sarre. 'Balancing Privacy with Legitimate Surveillance and Lawful Data Access'. *IEEE Cloud Computing* 2, no. 4 (July 2015): 8–13. https://doi.org/10.1109/MCC.2015.84.

Coates, Anthony Joseph. *The Ethics of War*. 2nd ed. Manchester: Manchester Univ. Press, 2016.

Cohen, Amichai, and David Zlotogorski. 'Incidental Harm and the Analysis of Proportionality'. In *Proportionality in International Humanitarian Law*, by Amichai Cohen and David Zlotogorski, 73–106. Oxford University Press, 2021. https://doi.org/10.1093/oso/9780197556726.003.0005.

Coverdale, John F. 'An Introduction to the Just War Tradition'. *Pace International Law Review* 16, no. 2 (September 2004): 221-78. https://digitalcommons.pace.edu/pilr/vol16/iss2/1

Crawford, Adam, ed. *Crime Prevention Policies in Comparative Perspective*. Cullompton, Devon; Portland, Or: Willan Pub, 2009.

Cuddihy, William J. *The Fourth Amendment: Origins and Original Meaning 602 - 1791*. 1st ed. Oxford University Press New York, 2009. https://doi.org/10.1093/acprof:oso/9780195367195.001.0001.

Daskal, Jennifer C. 'Pre-Crime Restraints: The Explosion of Targeted, Noncustodial Prevention'. *CORNELL LAW REVIEW* 99 (January 2014): 327-385.

De Brabandere, Eric. 'The Impact of Supranationalism on State Sovereignty from the Perspective of the Legitimacy of International Organisations'. In *Statehood and Self-Determination*, edited by Duncan French, 1st ed., 450–70. Cambridge University Press, 2013. https://doi.org/10.1017/CBO9781139248952.024.

Dencik, Lina, Arne Hintz, and Jonathan Cable. 'Towards Data Justice: Bridging Anti-Surveillance and Social Justice Activism 1'. In *Data Politics*. Routledge, 2019.

Dicey, A. V. *Introduction to the Study of the Law of the Constitution*. Indianapolis: Liberty/Classics, 1982.

Dothan, Shai. 'Judicial Tactics in the European Court of Human Rights'. *Chicago Journal of International Law* 12, no. 1 (2011): 115–41.

Dworkin, Gerald. *The Theory and Practice of Autonomy*. Cambridge University Press, 1988.

Eberle, Edward J. 'The Method and Role of Comparative Law'. *Washington University Global Studies Law Review* 8, no. 3 (1 January 2009): 451–86.

Ekelöf, Per Olof, Simon Andersson, Henrik Bellander, Torleif Bylund, Henrik Edelstam, and Mikael Pauli. *Rättegång. 3*. Åttonde upplagan. Institutet för Rättsvetenskaplig Forskning 27. Stockholm: Norstedts Juridik, 2018.

Ericson, Richard. 'Security, Surveillance and Counter-Law'. *Criminal Justice Matters* 68, no. 1 (June 2007): 6–7. https://doi.org/10.1080/09627250708553271.

Ericson, Richard V. ‘The State of Preemption: Managing Terrorism through Counter Law’. In *Risk and the War on Terror*, 1st ed., 57–76. London: Routledge, 2008.

Fabre, Cécile. *Spying through a Glass Darkly: The Ethics of Espionage and Counter-Intelligence*. First edition. New Topics in Applied Philosophy. Oxford: University Press, 2022.

Fellmeth, Aaron X., and Maurice Horwitz. ‘Nullum Crimen Sine Lege’. In *Guide to Latin in International Law*. Oxford University Press, 2022. https://www.oxfordreference.com/display/10.1093/acref/9780197583104.001.0001/acref-9780197583104-e-1541.

Ferguson, Pamela R. ‘The Presumption of Innocence and Its Role in the Criminal Process’. *Criminal Law Forum* 27, no. 2 (1 June 2016): 131–58. https://doi.org/10.1007/s10609-016-9281-8.

Finn, Rachel L., David Wright, and Michael Friedewald. ‘Seven Types of Privacy’. In *European Data Protection: Coming of Age*, edited by Serge Gutwirth, Ronald Leenes, Paul de Hert, and Yves Poullet, 3–32. Dordrecht: Springer Netherlands, 2013. https://doi.org/10.1007/978-94-007-5170-5_1.

Flyghed, Janne. ‘Normalising the Exceptional: The Case of Political Violence’. *Policing and Society* 13, no. 1 (January 2002): 23–41. https://doi.org/10.1080/1043946022000005608.

Freeden, Michael, and Emeritus Professor of Politics Michael Freeden. *Ideology: A Very Short Introduction*. OUP Oxford, 2003.

Friedman, Barry. ‘What Is Public Safety?’ SSRN Scholarly Paper. Rochester, NY, 8 February 2021. https://papers.ssrn.com/abstract=3808187.

Galetta, Antonella, and Paul De Hert. ‘Complementing the Surveillance Law Principles of the ECtHR with Its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance’. *Utrecht Law Review* 10, no. 1 (31 January 2014): 55. https://doi.org/10.18352/ulr.257.

Galetta, Antonella, and Paul de Hert. ‘Effects of Surveillance on the Rule of Law, Due Process and the Presumption of Innocence’. In *Surveillance in Europe*, edited by D. Wright and R. Kreissl, 283–91. Routledge, 2015.

Garland, David. *The Culture of Control: Crime and Social Order in Contemporary Society*. OUP Oxford, 2001.

Gendron, Angela. ‘Just War, Just Intelligence: An Ethical Framework for Foreign Espionage’. *International Journal of Intelligence and CounterIntelligence* 18, no. 3 (1 October 2005): 398–434. https://doi.org/10.1080/08850600590945399.

Gerards, Janneke. ‘How to Improve the Necessity Test of the European Court of Human Rights’. *International Journal of Constitutional Law* 11, no. 2 (1 April 2013): 466–90. https://doi.org/10.1093/icon/mot004.

Goold, B. J., and Liora Lazarus. *Security and Human Rights*. Oxford: Hart, 2007.

Goold, Benjamin J. ‘How Much Surveillance Is Too Much? Some Thoughts on Surveillance, Democracy, and the Political Value of Privacy’, n.d., 12.

Grabenwarter, Christoph. *European Convention on Human Rights: Commentary*. Bloomsbury Academic, 2013. https://doi.org/10.5040/9781472561725.

Greer, Steven. *The Exceptions to Articles 8 to 11 of the European Convention on Human Rights*. Human Rights Files 15. Strasbourg: Council of Europe Publ, 1997.

Guillaume, G. ‘The Use of Precedent by International Judges and Arbitrators’. *Journal of International Dispute Settlement* 2, no. 1 (1 February 2011): 5–23. https://doi.org/10.1093/jnlids/idq025.

Habermas, Jürgen. *The Structural Transformation of the Public Sphere: An Inquiry Into a Category of Bourgeois Society*. John Wiley & Sons, 2015.

Habermas, Jürgen, Jürgen Habermas, and Jürgen Habermas. *Reason and the Rationalization of Society*. Repr. The Theory of Communicative Action / Jürgen Habermas 1. Boston, Mass: Beacon Pr, 2007.

Hafetz, Jonathan. ‘Military Detention in the “War on Terrorism”: Normalizing the Exceptional After 9/11’. SSRN Scholarly Paper. Rochester, NY, 16 March 2012. https://papers.ssrn.com/abstract=2025057.

Haggerty, Kevin D., and Minas Samatas. *Surveillance and Democracy*. A Glasshouse Book. New York: Routledge, 2010. https://doi.org/10.4324/9780203852156.

Hall, Jerome. ‘Nulla Poena Sine Lege’. *The Yale Law Journal* 47, no. 2 (December 1937): 165. https://doi.org/10.2307/791967.

Heuman, Lars. ‘Vilka beviskrav gäller eller bör gälla för användningen av tvångsmedel?’ *Svensk Juristtidning*, no. 1 (2007): s. 141-53.

Hirst, Phoebe. ‘Mass Surveillance in the Age of Terror: Bulk Powers in the “Investigatory Powers Act 2016”’. *EUROPEAN HUMAN RIGHTS LAW REVIEW*, no. 4 (August 2019): 403–21. https://doi.org/10.3316/agispt.20190827016044.

Hjertstedt, Mattias, and Lena Landström. 'Domstolsprövning vid tvångsmedelsanvändning: En analys av rättighetsskyddet vid frihetsberövande och reell husrannsakan'. *Svensk juristtidning*, no. 8 (2020): 665–91.

Holvast, Jan. 'History of Privacy'. In *The Future of Identity in the Information Society*, edited by Vashek Matyáš, Simone Fischer-Hübner, Daniel Cvrček, and Petr Švenda, 298:13–42. IFIP Advances in Information and Communication Technology. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. https://doi.org/10.1007/978-3-642-03315-5_2.

Hosein, Gus. 'On Just Surveillance'. *Surveillance & Society* 12, no. 1 (12 March 2014): 154–57. https://doi.org/10.24908/ss.v12i1.5195.

Hradilova Selin, Klara, *Dödligt skjutvapenvåld i Sverige och andra europeiska länder: en jämförande studie av nivåer, trender och våldsmetoder, Brottsförebyggande rådet* (BRÅ 2021:8), Stockholm, 2021.

Huq, Aziz Z. 'Terrorism and Democratic Recession'. *The University of Chicago Law Review* 85, no. 2 (2018): 457–84.

HusabØ, Erling Johannes. 'Counterterrorism and the Expansion of Proactive Police Powers in the Nordic States'. *Journal of Scandinavian Studies in Criminology and Crime Prevention* 14, no. 1 (May 2013): 3–23. https://doi.org/10.1080/14043858.2013.773759.

James, Nick, and Kelley Burton. 'Measuring the Critical Thinking Skills of Law Students Using a Whole-of-Curriculum Approach'. *Legal Education Review* 27, no. 1 (1 January 2017). https://doi.org/10.53300/001c.6087.

Johnson, Deborah G, and Kent A Wayland. *Surveillance and Transparency as Sociotechnical Systems of Accountability*. Edited by Kevin D. Haggerty and Minas Samatas. *Surveillance and Democracy*. Routledge-Cavendish, 2010. https://doi.org/10.4324/9780203852156-8.

Joris, Tony, and Jan Vandenberghe. 'The Council of Europe and the European Union: Natural Partners or Uneasy Bedfellows?' *The Columbia Journal of European Law* 15, no. 1 (2009): 1–41.

Kant, Immanuel. *Practical Philosophy*. Cambridge University Press, 1999.

Keller, Helen, and Alec Stone Sweet. *A Europe of Rights: The Impact of the ECHR on National Legal Systems*. Oxford: University Press, 2016.

Kennedy, Duncan. 'The Structure of Blackstone's Commentaries'. *Buffalo Law Review* 28, no. 2 (1979 1978): 205–382.

Kilkelly, Ursula. *The Right to Respect for Private and Family Life: A Guide to the Implementation of Article 8 of the European Convention on Human Rights*. Directorate General of Human Rights, Council of Europe, 2001.

Killander, Magnus. 'Interpreting Regional Human Rights Treaties'. SSRN Scholarly Paper. Rochester, NY, 6 September 2011. https://papers.ssrn.com/abstract=1923206.

Klamberg, Mark. 'FRA and the European Convention on Human Rights: A Paradigm Shift in Swedish Electronic Surveillance Law'. In *Overvåking i En Rettstat*. Nordisk Årbok i Rettsinformatikk, 2010.

Kohl, Uta. 'Data Protection Law Revealed: The Right to Be Forgotten and Two Western Cultures of Privacy'. *SSRN Electronic Journal*, 2023. https://doi.org/10.2139/ssrn.4339695.

Königs, Peter. 'Government Surveillance, Privacy, and Legitimacy'. *Philosophy & Technology* 35, no. 1 (March 2022): 8. https://doi.org/10.1007/s13347-022-00503-9.

Kramer, Rory, and Brianna Remster. 'Stop, Frisk, and Assault? Racial Disparities in Police Use of Force During Investigatory Stops'. *Law & Society Review* 52, no. 4 (2018): 960–93. https://doi.org/10.1111/lasr.12366.

Lacey, Nicola. '5 Explaining the Shifting Alignment of Ideas of Responsibility in the Vortex of Interests and Institutions: Towards a Political Economy of Responsibility in English Criminal Law', n.d., 25.

Lachmayer, Konrad, and Normann Witzleb. 'The Challenge to Privacy from Ever Increasing State Surveillance: A Comparative Perspective'. *University of New South Wales Law Journal* 37, no. 2 (2014): 748–83. https://doi.org/10.3316/agis_archive.20142697.

Lamer, Wiebke. 'From Sleepwalking into Surveillance Societies to Drifting into Permanent Securitisation: Mass Surveillance, Security and Human Rights in Europe', December 2017. https://doi.org/20.500.11825/422.

Landau, Susan. *Surveillance or Security?: The Risks Posed by New Wiretapping Technologies*. MIT Press, 2011.

Landström, Lena. 'Hemliga tvångsmedel i brottsutredande syfte - Vem kan säga nej?' *Tidskrift (Suomen Lainopillinen Yhdistys)*, no. 5–6 (2015): 493-509.

Lappi-Seppälä, Tapio, and Michael Tonry. 'Crime, Criminal Justice, and Criminology in the Nordic Countries'. *Crime and Justice* 40, no. 1 (August 2011): 1–32. https://doi.org/10.1086/660822.

Lauren, Paul Gordon. 'The Foundations of Justice and Human Rights in Early Legal Texts and Thought'. In *The Oxford Handbook of International Human Rights Law*, edited by Dinah Shelton, 1st ed., 163–93. Oxford University Press, 2013. https://doi.org/10.1093/law/9780199640133.003.0008.

Law, Jonathan, ed. *A Dictionary of Law*. 10th ed. Oxford University Press, 2022. https://doi.org/10.1093/acref/9780192897497.001.0001.

Lazarus, Liora. 'Positive Obligations and Criminal Justice: Duties to Protect or Coerce?' In *Principles and Values in Criminal Law and Criminal Justice*, edited by Lucia Zedner and Julian V. Roberts, 135–56. Oxford University Press, 2012. https://doi.org/10.1093/acprof:oso/9780199696796.003.0009.

Lincoln, Denzin &. *The SAGE Handbook of Qualitative Research*. SAGE, 2005.

Lindberg, Gunnel. *Straffprocessuella Tvångsmedel: När och hur får de användas?* 5th ed. Stockholm, 2022.

Locke, John, and Richard Howard Cox. *Second Treatise of Government*. Crofts Classics. Arlington Heights, Ill: H. Davidson, 1982.

Loftus, Bethan, and Benjamin Goold. 'Covert Surveillance and the Invisibilities of Policing'. *Criminology & Criminal Justice* 12, no. 3 (July 2012): 275–88. https://doi.org/10.1177/1748895811432014.

Lührmann, Anna, and Staffan I. Lindberg. 'A Third Wave of Autocratization Is Here: What Is New about It?' *Democratization* 26, no. 7 (3 October 2019): 1095–1113. https://doi.org/10.1080/13510347.2019.1582029.

Lustgarten, Laurence, and I. Leigh. *In from the Cold: National Security and Parliamentary Democracy*. Oxford: New York: Clarendon Press; Oxford University Press, 1994.

Lyon, David. 'Surveillance after September 11'. *Sociological Research Online* 6, no. 3 (November 2001): 116–21. https://doi.org/10.5153/sro.643.

Lyon, David. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London; Routledge, 2003. https://doi.org/10.4324/9780203994887.

Lyon, David. 'Surveillance Studies: Understanding Visibility, Mobility and the Phenetic Fix.' *Surveillance & Society* 1, no. 1 (1 September 2002): 1–7. https://doi.org/10.24908/ss.v1i1.3390.

Lyon, David, Kevin D. Haggerty, and Kirstie Ball, eds. *Routledge Handbook of Surveillance Studies*. Abingdon, Oxon; New York: Routledge, 2012.

M. Kinsella, Helen. ‘Superfluous Injury and Unnecessary Suffering: National Liberation and the Laws of War’. In *Political Power and Social Theory*, edited by Tarak Barkawi and George Lawson, 32:205–31. Emerald Publishing Limited, 2017. https://doi.org/10.1108/S0198-871920170000032008.

Macnish, Kevin. ‘An Eye for an Eye: Proportionality and Surveillance’. *Ethical Theory and Moral Practice* 18, no. 3 (June 2015): 529–48. https://doi.org/10.1007/s10677-014-9537-5.

Macnish, Kevin. ‘Just Surveillance? Towards a Normative Theory of Surveillance’. *Surveillance & Society* 12, no. 1 (1 March 2014): 142–53. https://doi.org/10.24908/ss.v12i1.4515.

Macnish, Kevin. ‘Surveillance Ethics: An Introduction to an Introduction’. In *Advances in Research Ethics and Integrity*, edited by Ron Iphofen and Dónal O’Mathúna, 9–16. Emerald Publishing Limited, 2021. https://doi.org/10.1108/S2398-601820210000008002.

Maguire, Mike. ‘Policing by Risks and Targets: Some Dimensions and Implications of Intelligence-led Crime Control’. *Policing and Society* 9, no. 4 (January 2000): 315–36. https://doi.org/10.1080/10439463.2000.9964821.

Manunta, Giovanni. ‘What Is Security?’ *Security Journal* 12, no. 3 (July 1999): 57–66. https://doi.org/10.1057/palgrave.sj.8340030.

Maras, Marie-Helen. ‘The Social Consequences of a Mass Surveillance Measure: What Happens When We Become the “Others”?’ *International Journal of Law, Crime and Justice* 40, no. 2 (April 2012): 65–81. https://doi.org/10.1016/j.ijlcj.2011.08.002.

Marrin, Stephen. ‘Homeland Security Intelligence: Just the Beginning’. *Journal of Homeland Security* (January 2003):1-11. https://www.academia.edu/3695760/Homeland_Security_Intelligence_Just_the_Beginning.

Martins, Bruno. ‘Drones, Technology, and the Normalization of Exceptionalism in Contemporary International Security’. *Nação e Defesa* 146 (1 April 2017): 37–48.

McCulloch, Jude, and Dean Wilson. *Pre-Crime: Pre-Emption, Precaution and the Future*. First Edition. Routledge Frontiers of Criminal Justice 28. London; New York: Routledge, 2016.

McGarrity, Nicola, Andrew Lynch, and George Williams, eds. *Counter-Terrorism and beyond: The Culture of Law and Justice after 9/11*. Routledge Research in Terrorism and the Law. Abingdon, Oxon; New York, N.Y: Routledge, 2010.

McMahan, Jeff. ‘Just War’. In *A Companion to Contemporary Political Philosophy*, edited by Robert E. Goodin, Philip Pettit, and Thomas W. Pogge. John Wiley & Sons, 2012.

Meiklejohn, Alexander. ‘The First Amendment Is an Absolute’. *The Supreme Court Review* 1961 (January 1961): 245–66. https://doi.org/10.1086/scr.1961.3108719.

Milanovic, Marko. ‘Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age’. *Harvard International Law Journal* 56 (2015): 66.

Mill, John Stuart, David Bromwich, George Kateb, and Jean Bethke Elshtain. *On Liberty*. Rethinking the Western Tradition. New Haven: Yale University Press, 2003.

Miller, Seumas. ‘Rethinking the Just Intelligence Theory of National Security Intelligence Collection and Analysis: The Principles of Discrimination, Necessity, Proportionality and Reciprocity’. *Social Epistemology* 35, no. 3 (4 May 2021): 211–31. https://doi.org/10.1080/02691728.2020.1855484.

Miller, Seumas, Milton C. Regan, and Patrick F. Walsh, eds. *National Security Intelligence and Ethics*. Studies in Intelligence. Abingdon, Oxon; New York, NY: Routledge, 2022.

Mitsilegas, Valsamis. ‘The Preventive Turn in European Security Policy: Towards a Rule of Law Crisis?’ In *EU Law in Populist Times*, edited by Francesca Bignami, 1st ed., 301–18. Cambridge University Press, 2020. https://doi.org/10.1017/9781108755641.011.

Mokrosinska, Dorota. ‘Privacy and Autonomy: On Some Misconceptions Concerning the Political Dimensions of Privacy’. *Law and Philosophy* 37, no. 2 (April 2018): 117–43. https://doi.org/10.1007/s10982-017-9307-3.

Møller, Jørgen, and Svend-Erik Skaaning. ‘Systematizing Thin and Thick Conceptions of the Rule of Law’. *Justice System Journal* 33, no. 2 (May 2012): 136–53. https://doi.org/10.1080/0098261X.2012.10768008.

Molnar, Adam. ‘Technology, Law, and the Formation of (Il)Liberal Democracy?’ *Surveillance & Society* 15, no. 3/4 (9 August 2017): 381–88. https://doi.org/10.24908/ss.v15i3/4.6645.

Monaghan, Jeffrey, and Kevin Walby. ‘Making up “Terror Identities”: Security Intelligence, Canada’s Integrated Threat Assessment Centre and Social Movement Suppression’. *Policing and Society* 22, no. 2 (June 2012): 133–51. https://doi.org/10.1080/10439463.2011.605131.

Monahan, Torin. ‘Editorial: Surveillance and Inequality’. *Surveillance and Society* 5 (1 January 2008).

Monahan, Torin. ‘Surveillance as Governance: Social Inequality and the Pursuit of Democratic Surveillance’. In *Surveillance and Democracy*, edited by Kevin D. Haggerty and Minas Samatas. Routledge-Cavendish, 2010.

Moore, Adam D. ‘Why Privacy and Accountability Trump Security’. *SSRN Electronic Journal*, 2015. https://doi.org/10.2139/ssrn.2673712.

Morgan, Nigel, and Annette Pritchard. ‘Security and Social “Sorting”: Traversing the Surveillance–Tourism Dialectic’. *Tourist Studies* 5, no. 2 (August 2005): 115–32. https://doi.org/10.1177/1468797605066923.

Murphy, Cian C. ‘EU Counter-Terrorism & the Rule of Law in a Post-“War on Terror” World’. SSRN Scholarly Paper. Rochester, NY, 26 April 2011. https://papers.ssrn.com/abstract=1958335.

Naarttijärvi, Markus. ‘För din och andras säkerhet: konstitutionella proportionalitetskrav och Säkerhetspolisens preventiva tvångsmedel’. Skrifter från Juridiska institutionen vid Umeå universitet, 29. Iustus, 2013.

Nagra, Baljit, and Paula Maurutto. ‘No-Fly Lists, National Security and Race: The Experiences of Canadian Muslims’. *The British Journal of Criminology* 60, no. 3 (4 April 2020): 600–619. https://doi.org/10.1093/bjc/azz066.

Nathan, Christopher. ‘Liability to Deception and Manipulation: The Ethics of Undercover Policing’. *Journal of Applied Philosophy* 34, no. 3 (May 2017): 370–88. https://doi.org/10.1111/japp.12243.

Nathan, Christopher. *The Ethics of Undercover Policing*. Routledge, 2022.

Nunn, Samuel. ‘Measuring Criminal Justice Technology Outputs: The Case of Title III Wiretap Productivity, 1987-2005’. *Journal of Criminal Justice* 36, no. 4 (August 2008): 344–53. https://doi.org/10.1016/j.jcrimjus.2008.06.006.

O’Donnell, Guillermo A. ‘Why the Rule of Law Matters’. *Journal of Democracy* 15, no. 4 (2004): 32–46. https://doi.org/10.1353/jod.2004.0076.

Omand, David, and Mark Phythian. *Principled Spying: The Ethics of Secret Intelligence*. Washington: Georgetown University Press, 2018. http://muse.jhu.edu/pub/171/monograph/book/59033.

Orwell, George, and Erich Fromm. *1984*. New York, New York, USA: Signet Classics, 2017.

Palmer, Phil. ‘Dealing with the Exceptional: Pre-Crime Anti-Terrorism Policy and Practice’. *Policing and Society* 22, no. 4 (December 2012): 519–37. https://doi.org/10.1080/10439463.2011.641549.

Penney, Jonathon W. ‘Chilling Effects: Online Surveillance and Wikipedia Use’, 2016. https://doi.org/10.15779/Z38SS13.

Petkova, Bilyana. ‘Privacy as Europe’s First Amendment’. *European Law Journal* 25, no. 2 (March 2019): 140–54. https://doi.org/10.1111/eulj.12316.

Piaseczny, Michael Joseph. ‘The Determinants of Differing Legislative Responses in Similar States: A Nordic Case Study’. *Mapping Politics* 9, no. 0 (11 September 2018). https://journals.library.mun.ca/ojs/index.php/MP/article/view/1889.

Piza, Eric L., Brandon C. Welsh, David P. Farrington, and Amanda L. Thomas. ‘CCTV Surveillance for Crime Prevention: A 40-year Systematic Review with Meta-analysis’. *Criminology & Public Policy* 18, no. 1 (February 2019): 135–59. https://doi.org/10.1111/1745-9133.12419.

Powell, Rhonda. *Rights as Security: The Theoretical Basis of Security of Person*. 1st ed. Oxford University Press, 2019. https://doi.org/10.1093/oso/9780199589111.001.0001.

Quinlan, Michael. ‘Just Intelligence: Prolegomena to an Ethical Theory’. *Intelligence and National Security* 22, no. 1 (1 February 2007): 1–13. https://doi.org/10.1080/02684520701200715.

Raab, Charles. ‘Surveillance: Effects on Privacy, Autonomy and Dignity’. *Surveillance in Europe*, October 2014, 259–68.

Regan, Priscilla M. *Legislating Privacy: Technology, Social Values, and Public Policy*. University of North Carolina Press, 1995.

Rengel, Alexandra. *Privacy in the 21st Century*. Studies in Intercultural Human Rights, volume 5. Leiden: Martinus Nijhoff Publishers, 2013.

Richards, Neil M. ‘THE DANGERS OF SURVEILLANCE’. *Harvard Law Review* 126, no. 7 (2013): 1934–65.

Riley, Jonathan. *Mill on Liberty*. Routledge Philosophy Guidebooks. London; New York: Routledge, 1998.

Roach, Kent. *The 9/11 Effect: Comparative Counter-Terrorism*. Cambridge University Press, 2011.

Robbins, Scott. ‘Bulk Data Collection, National Security and Ethics’. In *Counter-Terrorism*, by Seumas Miller, Adam Henschke, and Jonas Feltes Feltes, 169–80. Edward Elgar Publishing, 2021. https://doi.org/10.4337/9781800373075.00020.

Rojszczak, Marcin. ‘Surveillance, Legal Restraints and Dismantling Democracy: Lessons from Poland’. *Democracy and Security* 17, no. 1 (2 January 2021): 1–29. https://doi.org/10.1080/17419166.2020.1841367.

Rønn, Kira Vrist, and Kasper Lippert-Rasmussen. 'Out of Proportion? On Surveillance and the Proportionality Requirement'. *Ethical Theory and Moral Practice* 23, no. 1 (February 2020): 181–99. https://doi.org/10.1007/s10677-019-10057-z.

Rusinova, Vera. 'A European Perspective on Privacy and Mass Surveillance at the Crossroads'. *SSRN Electronic Journal*, 2019. https://doi.org/10.2139/ssrn.3347711.

Sajó, András, and Renáta Uitz. *The Constitution of Freedom: An Introduction to Legal Constitutionalism*. Oxford, United Kingdom: Oxford University Press, 2017.

Sassòli, Marco. *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare*. Edward Elgar Publishing, 2019.

Schabas, William. *The European Convention on Human Rights: A Commentary*. First edition. Oxford Commentaries on International Law. Oxford, United Kingdom: Oxford University Press, 2015.

Scheppele, Kim. 'Autocratic Legalism'. *University of Chicago Law Review* 85, no. 2 (1 March 2018). https://chicagounbound.uchicago.edu/uclrev/vol85/iss2/2.

Schulzke, Marcus. *Just War Theory and Civilian Casualties: Protecting the Victims of War*. Cambridge University Press, 2017.

Schweden, ed. *Riksdagens flerspråkiga ordlista: vanliga termer i riksdagens arbete och EU-samarbetet i översättning till engelska, franska och tyska*. Stockholm: Sveriges riksdag, 2015.

Sedgwick, Mark. 'The Concept of Radicalization as a Source of Confusion'. *Terrorism and Political Violence* 22, no. 4 (14 September 2010): 479–94. https://doi.org/10.1080/09546553.2010.491009.

Selinger, Evan, and Hyo Joo (Judy) Rhee. 'Normalizing Surveillance'. *SATS* 22, no. 1 (27 July 2021): 49–74. https://doi.org/10.1515/sats-2021-0002.

Setty, Sudha. 'Surveillance and the Inversion of Democratic Transparency'. In *Routledge Handbook of Democracy and Security*, edited by Leonard Weinberg, Elizabeth Francis, and Eliot Assoudeh, 1st ed., 28–39. Routledge, 2020. https://doi.org/10.4324/9781315755724-2.

Shor, Eran, Ina Filkobski, Pazit Ben-Nun Bloom, Hayder Alkilabi, and William Su. 'Does Counterterrorist Legislation Hurt Human Rights Practices? A Longitudinal Cross-National Analysis'. *Social Science Research* 58 (July 2016): 104–21. https://doi.org/10.1016/j.ssresearch.2015.12.007.

Siems, Mathias. *Comparative Law*. Cambridge University Press, 2022.

Skinnari, Johanna, Stenström, Anders & Korsell, Lars, *Otillåten påverkan mot företag: en undersökning om utpressning*, Brottsförebyggande rådet (BRÅ 2012:12), Stockholm, 2012.

Slobogin, Christopher, and Sarah Brayne. 'Surveillance Technologies and Constitutional Law'. *Annual Review of Criminology* 6, no. 1 (27 January 2023): 219–40. https://doi.org/10.1146/annurev-criminol-030421-035102.

Smith, Richard. 'The Margin of Appreciation and Human Rights Protection in the 'War on Terror': Have the Rules Changed before the European Court of Human Rights?' *Essex Human Rights Review* 8(1) (2011): 124–53.

Solove, Daniel, and Danielle Keats Citron. 'Privacy Harms'. *GW Law Faculty Publications & Other Works*, 1 January 2021. https://scholarship.law.gwu.edu/faculty_publications/1534.

Solove, Daniel J. 'Conceptualizing Privacy'. *California Law Review* 90, no. 4 (2002): 1087–1156.

Solove, Daniel J. *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven: Yale University Press, 2014.

Sorell, Tom. 'Preventive Policing, Surveillance, and European Counter-Terrorism'. *Criminal Justice Ethics* 30, no. 1 (April 2011): 1–22. https://doi.org/10.1080/0731129X.2011.559057.

Spapens, Toine. 'Interaction between Criminal Groups and Law Enforcement: The Case of Ecstasy in the Netherlands'. *Global Crime* 12, no. 1 (15 February 2011): 19–40. https://doi.org/10.1080/17440572.2011.548955.

Staden, A. von. 'The Democratic Legitimacy of Judicial Review beyond the State: Normative Subsidiarity and Judicial Standards of Review'. *International Journal of Constitutional Law* 10, no. 4 (1 October 2012): 1023–49. https://doi.org/10.1093/icon/mos032.

Steiker, Carol S. 'The Limits of the Preventive State. (Supreme Court Review)'. *The Journal of Criminal Law & Criminology* 88, no. 3 (1998): 771–808.

Steinhoff, Uwe. *On the Ethics of War and Terrorism*. Oxford; New York: Oxford University Press, 2007.

Stoddart, Eric. 'Challenging "Just Surveillance Theory": A Response to Kevin Macnish's "Just Surveillance? Towards a Normative Theory of Surveillance"'. *Surveillance & Society* 12, no. 1 (12 March 2014): 158–63. https://doi.org/10.24908/ss.v12i1.5196.

Stoughton, Seth W., Kyle McLean, Justin Nix, and Geoffrey Alpert. 'Policing Suspicion: Qualified Immunity and "Clearly Established" Standards of Proof'. *CrimRxiv*, 9 July 2021. https://doi.org/10.21428/cb6ab371.ccfee09e.

Strandh, Veronica, and Niklas Eklund. 'Swedish Counterterrorism Policy: An Intersection Between Prevention and Mitigation?' *Studies in Conflict & Terrorism* 38, no. 5 (4 May 2015): 359–79. https://doi.org/10.1080/1057610X.2015.1009799.

Susser, Daniel. 'Data and the Good?' *Surveillance and Society* 20, no. 3 (2022): 297–301.

Szeghalmi, Veronika. 'The Definition of the Right to Privacy in the United States of America and Europe Part III Developments in International Law'. *Hungarian Yearbook of International Law and European Law* 2015 (2015): 397–410.

Tamanaha, Brian Z. 'A Concise Guide to the Rule of Law'. SSRN Scholarly Paper. Rochester, NY, 13 September 2007. https://papers.ssrn.com/abstract=1012051.

Taylor, Nick. 'To Find the Needle Do You Need the Whole Haystack? Global Surveillance and Principled Regulation'. *The International Journal of Human Rights* 18, no. 1 (2 January 2014): 45–67. https://doi.org/10.1080/13642987.2013.871109.

Thimm, Johannes. 'From Exception to Normalcy: The United States and the War on Terrorism'. *7/2018* 7/2018 (2018): 39.

Tsakyrakis, S. 'Proportionality: An Assault on Human Rights?' *International Journal of Constitutional Law* 7, no. 3 (1 July 2009): 468–93. https://doi.org/10.1093/icon/mop011.

Turner, Ian. 'A Positive, Communitarian Right to Security in the Age of Super-Terrorism'. *Democracy and Security* 13, no. 1 (2 January 2017): 46–70. https://doi.org/10.1080/17419166.2016.1242420.

Utset, Manuel A. 'Digital Surveillance and Preventive Policing'. SSRN Scholarly Paper. Rochester, NY, 1 September 2017. https://papers.ssrn.com/abstract=3205520.

Van Brakel, Rosamunde. 'The Rise of Preemptive Surveillance of Children in England: Unintended Social and Ethical Consequences'. In *Surveillance Futures: Social and Ethical Implications of New Technologies for Children and Young People*. Abingdon, Oxon; New York: Routledge, 2017.

Van Brakel, Rosamunde, and Paul Hert. 'Policing, Surveillance and Law in a Pre-Crime Society: Understanding the Consequences of Technology Based Strategies'. *Journal of Police Studies* 20 (1 January 2011): 163–92.

Van der Sloot, Bart. 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of Big Data Research Article'. *Utrecht Journal of International and European Law* 31, no. 80 (2015): 25–50.

Vasilopoulos, Pavlos, George E. Marcus, and Martial Foucault. 'Emotional Responses to the Charlie Hebdo Attacks: Between Ideology and Political Judgment'. *SSRN Electronic Journal*, 2015. https://doi.org/10.2139/ssrn.2693952.

Versteeg, Mila, and Tom Ginsburg. 'Measuring the Rule of Law: A Comparison of Indicators'. *Law & Social Inquiry* 42, no. 01 (2017): 100–137. https://doi.org/10.1111/lsi.12175.

Vervaele, John A. E. 'Surveillance and Criminal Investigation: Blurring of Thresholds and Boundaries in the Criminal Justice System?' In *Reloading Data Protection*, edited by Serge Gutwirth, Ronald Leenes, and Paul De Hert, 115–28. Dordrecht: Springer Netherlands, 2014. https://doi.org/10.1007/978-94-007-7540-4_7.

Vranken, Jan. 'Exciting Times for Legal Scholarship'. *Law and Method* 2, no. 2 (2012): 42–62. https://doi.org/10.5553/ReM/221225082012002002004.

Vrist Ronn, Kira. 'Intelligence Ethics: A Critical Review and Future Perspectives'. *International Journal of Intelligence and CounterIntelligence* 29, no. 4 (October 2016): 760–84. https://doi.org/10.1080/08850607.2016.1177399.

Waldron, Jeremy. *Torture, Terror, and Trade-Offs: Philosophy for the White House*. OUP Oxford, 2012.

Wallerstein, Shlomit. 'On the Legitimacy of Imposing Direct and Indirect Obligations to Disclose Information on Non-Suspects'. In *Seeking Security: Pre-Empting the Commission of Criminal Harms*, edited by G. R. Sullivan and I. H. Dennis. Oxford; Portland, Or: Hart Pub, 2012.

Wallin, Lisa, Skinnari, Johanna & Korsell, Lars, *Utpressning i Sverige: tvistelösning, bestraffning och affärsidé*, Brottsförebyggande rådet (BRÅ 2012:6), Stockholm, 2012.

Weber, Rolf H., and Dominic N. Staiger. 'Bridging the Gap between Individual Privacy and Public Security', 2014. https://doi.org/10.5167/UZH-108655.

Westin, Alan F. 'How the Public Sees the Security-versus-Liberty Debate'. In *Protecting What Matters*. Brookings Institution Press, 2007. https://doi.org/10.7864/j.ctt1gpccs0.6.

Westin, Alan F. *Privacy and Freedom*. New York: Atheneum for the Assoc. of the Bar of the City of New York, 1967.

Wilkinson, J. Harvie. 'THE PRESUMPTION OF CIVIL INNOCENCE'. *Virginia Law Review* 104, no. 4 (2018): 589–653.

Yesufu, Shaka. 'Discriminatory Use of Police Stop-and-Search Powers in London, UK'. *International Journal of Police Science & Management* 15, no. 4 (December 2013): 281–93. https://doi.org/10.1350/ijps.2013.15.4.318.

Zarbiyev, F. 'Judicial Activism in International Law--A Conceptual Framework for Analysis'. *Journal of International Dispute Settlement* 3, no. 2 (1 July 2012): 247–78. https://doi.org/10.1093/jnlids/ids005.

Zedner, Lucia, and Andrew Ashworth. 'The Rise and Restraint of the Preventive State'. *Annual Review of Criminology* 2, no. 1 (13 January 2019): 429–50. https://doi.org/10.1146/annurev-criminol-011518-024526.

Internet Sources

9/11 Commission. 'National Commission on Terrorist Attacks Upon the United States Twelfth Public Hearing'. Washington, D.C.: National Commission on Terrorist Attacks Upon the United States, 16 June 2004. https://govinfo.library.unt.edu/911/archive/hearing12/9-11Commission_Hearing_2004-06-16.htm.

Amnesty International. 'Georgia Archives'. Amnesty International. Accessed 4 November 2022.https://www.amnesty.org/en/location/europe-and-central-asia/georgia/report-georgia/.

Auten, Brian. 'Examining Just Intelligence Theory'. The Political Theology Network, 25 September 2013. https://politicaltheology.com/examining-just-intelligence-theory/.

Babuta, Alexander, and Marion Oswald. 'Data Analytics and Algorithmic Bias in Policing'. *The Royal United Services Institute for Defence and Security Studies*, 2019. https://static.rusi.org/20190916_data_analytics_and_algorithmic_bias_in_policing_web_0.pdf.

Ball, James. 'NSA Monitored Calls of 35 World Leaders after US Official Handed over Contacts'. *The Guardian*, 25 October 2013, sec. US news. https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls.

Civil Rights Defenders. 'Serious Criticism Against Proposal on Wiretapping Without Crime Suspicion'. *Civil Rights Defenders*, 4 November 2021. https://crd.org/2021/11/04/serious-criticism-against-proposal-on-wiretapping-without-criminal-suspicion/.

Council of Europe. 'Map & Members'. Council of Europe Office in Georgia. Accessed 9 November 2022. https://www.coe.int/en/web/tbilisi/the-coe/objectives-and-missions.

Courts of Sweden. *Svensk/Engelsk, Engelsk/Svensk Ordlista För Sveriges Domstolar = Swedish/English, English/Swedish Glossary for the Courts of Sweden*. 5th ed. Stockholm: AJ E-print AB, 2019. https://www.domstol.se/om-sveriges-domstolar/for-dig-som-aktor-i-domstol/stod-for-aktorer-i-domstol/ordlistor/svenskengelsk-ordlista-for-sveriges-domstolar/.

DCAF. *Counterintelligence and Law Enforcement Functions in the Intelligence Sector*. Vol. 2020. Geneva Centre for Security Sector Governance, 2020. Accessed 13 December 2022.https://www.dcaf.ch/sites/default/files/publications/documents/CounterintelligenceLawEnforcementFunctionsIntelligenceSector.pdf.

DCAF. *Intelligence Services Roles and Responsibilities in Good Security Sector Governance*. Vol. 2015. SSR Backgrounder. Geneva: Geneva Centre for the Democratic Control of Armed Forces. Accessed 13 December 2022. https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_12_Intelligence%20Services.pdf.

Economist Intelligence. 'Democracy Index 2021: The China Challenge', 2021. Accessed 13 December 2022.https://www.eiu.com/n/campaigns/democracy-index-2021/.

European Commission on Democracy through Law (Venice Commission), *Resolution RES (2002) 3 Adopting the Revised Statute of the European Commission for Democracy through Law*, CDL (2002)027-e, Strasbourg, 27 February 2002. Accessed 18 November 2022. https://www.venice.coe.int/WebForms/documents/?pdf=CDL(2002)027-e&lang=EN.

European Commission for Democracy through Law (Venice Commission), *Report on the Rule of Law - Adopted by the Venice Commission at its 86th plenary session (Venice, 25-26 March 2011)*, Study No. 512/ 2009, CDL-AD (2011) 003 rev., Strasbourg, 4 April 2011. Accessed 18 November 2022. https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2011)003rev-e.

Eriksson, Niklas, and Ebba Thornéus. 'Regeringens 34 punkter för att stoppa gängvåldet: Massivt'. *Aftonbladet*, 21 September 2019. https://www.aftonbladet.se/a/y3XK0r.

European Union Agency for Fundamental Rights. *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II, Field Perspectives and Legal Update.* LU: Publications Office, 2017. https://data.europa.eu/doi/10.2811/792946.

European Commission on Democracy through Law (Venice Commission), *Rule of Law Checklist Adopted by the Venice Commission at its 106th Plenary Session (Venice, 11-12 March 2016)*, CDL-AD (2016)007, Strasbourg, 18 March 2016.Accessed 18 November 2022. https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2016)007-e.

European Commission on Democracy through Law (Venice Commission), *Urgent Joint Opinion of the Venice Commission and the Directorate General of Human Rights and Rule of Law (DGI) of the Council of Europe on amendments to the Law on the Common courts, the Law on the Supreme court and some other Laws, issued pursuant to Article 14a of the Venice Commission's Rules of Procedure on 16 January 2020, endorsed by the Venice Commission on 18 June by a written procedure replacing the 123rd Plenary Session*, CDL-AD(2020)017, Strasbourg, 22 June 2020. Accessed 18 November 2022. Venice Commission: Council of Europe (coe.int).

European Commission on Democracy through Law (Venice Commission), *Opinion on the Act of 15 January 2016 amending the Police Act and certain other Acts, adopted by the Venice Commission at its 107th Plenary Session (Venice, 10-11 June 2016)*, CDL-AD(2016)012-e, Strasbourg, 13 June. Accessed 18 November 2022.Venice Commission: Council of Europe (coe.int).

Fife, Robert. 'Up to 100,000 Canadians Could Be Affected by No-Fly List, Research Suggests - The Globe and Mail'. *The Globe and Mail*, 11 December 2017. https://www.theglobeandmail.com/news/politics/up-to-100000-canadians-could-wrongly-be-on-no-fly-list-research-suggests/article37299604/.

Government of Sweden. 'Statement of Government Policy', 18 October 2022. https://www.government.se/4abdb6/contentassets/9c187813e7b3488ea595c9e28e2411e5/statement-of-government-policy-2022-eng.pdf.

ICRC. 'Customary Law'. Topic. International Committee of the Red Cross, 28 July 2014. https://www.icrc.org/en/war-and-law/treaties-customary-law/customary-law.

ICRC. 'ICRC's Study on Customary International Humanitarian Law (IHL)'. International Committee of the Red Cross. Accessed 15 November 2022. https://ihl-databases.icrc.org/customary-ihl/eng/docs/home.

ICRC. 'International Rules and Standards for Policing'. Geneva, June 2015.

ICRC. ‘Treaties, States Parties, and Commentaries - States Parties - Convention (IV) Relative to the Protection of Civilian Persons in Time of War. Geneva, 12 August 1949.’ International Committee of the Red Cross. Accessed 28 November 2022. https://ihldatabases.icrc.org/applic/ihl/ihl.nsf/States.xsp?xp_viewStates=XPages_NORMStatesParties&xp_treatySelected=380.

INCLO. ‘Spying on Dissent Surveillance Technologies and Protest’, 1 June 2019. https://www.inclo.net/publications/

INCLO. ‘Surveillance and Democracy: Chilling Tales from Around the World’. 11 October 2016.https://www.inclo.net/publications/

International Commission on Intervention and State Sovereignty, Gareth J. Evans, Mohamed Sahnoun, and International Development Research Centre (Canada), eds. *The Responsibility to Protect: Report of the International Commission on Intervention and State Sovereignty*. Ottawa: International Development Research Centre, 2001.

International Service for Human Rights. ‘China’s Abuse of National Security to Curtail Human Rights: 4 Things You Need to Know’. ISHR, 27 January 2022. https://ishr.ch/latest-updates/chinas-abuse-of-national-security-to-curtail-human-rights-4-things-you-need-to-know/.

Klamberg, Mark. ‘Big Brother’s Little, More Dangerous Brother’. *Verfassungsblog: On Matters Constitutional*, 1 June 2021. https://doi.org/10.17176/20210601-123800-0.

Mazzini, Martina, and Ottavio Marzocchi. ‘Pegasus and Surveillance Spyware’. Brussels: Policy Department for Citizens’ Rights and Constitutional Affairs, May 2022. http://www.europarl.europa.eu/supporting-analyses.

No Fly List Kids. ‘100k Canadians – #NoFlyListKids’. No Fly List Kids. Accessed 3 February 2023. https://noflylistkids.ca/en/100000-canadians/.

Pilkington, Ed. ‘NYPD Settles Lawsuit after Illegally Spying on Muslims’. *The Guardian*, 5 April 2018, sec. World news. https://www.theguardian.com/world/2018/apr/05/nypd-muslim-surveillance-settlement.

Polismyndigheten. ‘Polismyndighetens kamerabevakning av platser dit allmänheten har tillträde’. Stockholm: Rikspolischefens kansli, December 2021. https://polisen.se/link/226f6df1d4aa4b63b05bea4d6e5d67ca.

Polismyndigheten. ‘Sprängningar och skjutningar’. polisen.se, 2022. https://polisen.se/link/4c9c6642003b48ac947dd3107370731c.

Ringgren, Helmer. ‘Qur’an | Description, Meaning, History, & Facts | Britannica’. Britannica, 21 August 2022. https://www.britannica.com/topic/Quran.

Stanley, Jay. ‘Six Questions to Ask Before Accepting a Surveillance Technology’. ACLU of Oregon, 15 August 2022. https://www.aclu-or.org/en/news/six-questions-ask-accepting-surveillance-technology.

Statement of Opinion, Institutet för mänskliga rättigheter, Dnr 1.1.2–283/2022, 9 September 2022. Accessed 9 February 2023. https://www.regeringen.se/4a5f46/contentassets/241b9f690afc4bea8b46c445f06d34b8/institutet-for-manskliga-rattigheter.pdf.

Statement of Opinion, Juridiska Fakultetsnämnden vid Uppsala Universitet, JURFAK 2022/26, 12 September 2022, Uppsala. Accessed 9 February 2023. https://www.jur.uu.se/digitalAssets/925/c_925232-l_3-k_jurfak2022_26.pdf.

Statement of Opinion, Sveriges Advokatsamfund, R-2022/1035, Stockholm, 14 September 2022. Accessed 9 February 2023. https://www.advokatsamfundet.se/globalassets/advokatsamfundet_sv/remissvar/utokade_mojligheter_att_anvanda_hemliga_tvangsmedel_sou_2022_19.pdf

Statement of Opinion, the Swedish Commission on Security and Integrity Protection, Dnr 87-2022, 21 September 2022.Accessed 9 February 2023. https://www.regeringen.se/4a7713/contentassets/241b9f690afc4bea8b46c445f06d34b8/sakerhets--och-integritetsskyddsnamnden.pdf.

Statement of Opinon, The Swedish Prosecution Authority, ÅM2022-1189, 1 November 2022.Accessed 9 February 2023. https://www.regeringen.se/remisser/2022/05/remiss-av-sou-202219-utokade-mojligheter-att-anvanda-hemliga-tvangsmedel/.

Sverigedemokraterna, Moderaterna, Kristdemokraterna, and Liberalerna. ‘Tidöavtalet: Överenskommelse För Sverige’. Accessed 2 January 2023. https://via.tt.se/data/attachments/00551/04f31218-dccc-4e58-a129-09952cae07e7.pdf.

Sveriges Radio. ‘Government Open for Secret Police Surveillance and House Searches without Concrete Suspicion’. *Sveriges Radio*, 12:59:00Z, sec. Radio Sweden. https://sverigesradio.se/artikel/government-open-for-secret-police-surveillance-and-house-searches-without-concrete-suspicion.

‘The Avalon Project: Code of Hammurabi’. Accessed 11 October 2022. https://avalon.law.yale.edu/ancient/hamframe.asp.

TT. ‘Hemliga tvångsmedel ska stoppa gängvåld’. *Aftonbladet*, 24 October 2022. https://www.aftonbladet.se/a/onnOx0.

UN Commission on Human Rights, *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, E/CN.4/1985/4, 28 September 1984. Accessed 19 November 2022. https://www.icj.org/siracusa-principles-on-the-limitation-and-derogation-provisions-in-the-international-covenant-on-civil-and-political-rights/.

UN Security Council, *The rule of law and transitional justice in conflict and post-conflict societies: report of the Secretary-General*, S/2004/616, 23 August 2004. Accessed 18 November 2022. https://www.securitycouncilreport.org/un-documents/document/pcs-s-2004-616.php.

UN. 'United Nations Treaty Collection'. United Nations Treaty Collection. Accessed 28 November 2022. https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=I-1&chapter=1&clang=_en.

Yang, Jennifer. 'G20 Law Gives Police Sweeping Powers to Arrest People'. *Toronto Star*, 25 June 2010. https://www.thestar.com/news/gta/g20/2010/06/25/g20_law_gives_police_sweeping_powers_to_arrest_people.html.

Yaroyvi, Olexander, Hauke Vagts, Sebastian Höhn, Gulijk Van, and Coen. 'SURVEILLE Deliverable 2.1: Survey of Surveillance Technologies, Including their specific Identification for further Work', 2012. https://surveille.eui.eu/wp-content/uploads/sites/19/2015/04/D2.1-Survey-of-surveillance-technologies.pdf.