National Security v. Personal Insecurity – Electronic Surveillance and Prevention of Abuse of State Power in U.S., Germany and Georgia

By

Tamari Samkharadze

Submitted to
Central European University
Department of Legal studies

Comparative Constitutional Law

Supervisor: Professor Alexander Blankenagel

Budapest, Hungary

2018

Table of contents

Abstract

This thesis examines and compares approaches towards the privacy v. security trade-off in the U.S., Germany and Georgia with the specific focus on the decisions of domestic Supreme/Constitutional Courts regarding the prevention of abuse of powers while conducting electronic surveillance. Discussion on the jurisprudence of the respective Courts demonstrates that despite American libertarian principles focusing on constraining the state power, in the context of electronic surveillance the Supreme Court has failed to address the contemporary challenges. By contrast, with the desire to overcome the inheritance of the totalitarian past, Constitutional Courts of Germany and Georgia have engaged in more meaningful Constitutional review, by expansive interpretation of scope of privacy, as well as their focus on the rule of law and elaborate system of safeguards.

Introduction

Information is power and thus, concentration of information amounts to a concentration of power.[1] In the wake of the fight against terrorism, natural inclination of the government to expand its powers is easier to justify by putting increased emphasis on threats to national security. Far-reaching possibilities of new surveillance techniques magnifies the risks of abuse of power to a dangerous degree. Advocates of the vast executive discretion call privacy a terminal disease for the effective government.[2] The proponents of privacy however, suggest that the trade-off between security and liberty need not necessarily be zero.[3] According to Daniel Solove, where intelligence programs coexist with the adequate oversight mechanisms and limitations on subsequent uses, accommodation of both interests could effectively be achieved in a balanced manner.[4]

Breaking free from the colonial rule, the primary purpose behind the fourth amendment in the U.S. as well as the Constitution itself has been to establish a limited state power.[5] In the book on Privacy and Freedom Alan F. Westin highlights that Americans have traditionally been suspicious of police and government officials and the fourth amendment was designed to prevent police omniscience as "one of the most effective tools of tyranny." Westin refers to expansive surveillance in "authoritarian systems" and "police government" that had been deliberately

[1] Westin, Alan. 2015. *Privacy and Freedom*. New York: Athenium. 299.
[2] Stuntz, William J. 2006. "Secret Service: Against Privacy and Transparency." *New Republic*, April 17, 2006
[3] Solove, Daniel J. 2008. Data Mining and the Security-Liberty Debate, *University of Chicago Law Review*, 75 (1): 343-362. 362.
[4] *ibid.*
[5] Gray, David C. 2017. *The Fourth Amendment in an age of surveillance*. Cambridge: Cambridge University Press. 69

rejected by U.S as contrary to American libertarian principles."[6] History of abuses however have demonstrated that without effective checks, temptation of using such tools are too hard to resist.

Having experienced the rule of continental "authoritarian systems," itself, Germany had to overcome the painful experience of oppressive regime and "disastrous abuses of the personal records."[7] Trying to distance itself from Horrors of Nazism, Post-War Basic Law established a new value-oriented constitutional order intending to reinstate the "centrality of humanity to the social order."[8] According to James Q. Whitman, unlike American understanding of freedom as being free from governmental intrusion, in Germany purpose of freedom is a possibility of individual self-realization.[9] Thus, Whitman argues that in contrast with American liberty-oriented perspective, the core of privacy protection in Germany emanates from the notion of personal dignity and free development of personality.[10]

Sharing a similar experience of systematic neglect of privacy rights during the repressive control of the Communist Regime, Georgia followed the example of post-war Germany with the aim to establish itself as a democratic state with respect for human rights.[11] Self-limited government, centrality of personality and the highest value of human dignity were recognized as the anchors of the new Constitution and the basis of the privacy protection as well.[12]

[6] Westin, 332, 358.
[7] Bignami, Francesca, 2007. European versus American Liberty, a Comparative Privacy Analysis of Antiterrorism Data Mining. *Boston College Law Review* 48, (3): 609-698. 610.
[8] Eberle J. Edward. 1997. Human Dignity, Privacy, and Personality in German and American Constitutional Law, *Utah Law Review*. 1997: 963-1056. 967.
[9] Whitman, James Q. 2004. The Two Western Cultures of Privacy: Dignity versus Liberty. *The Yale Law Journal* 113, (6): 1151-1221. 1181.
[10] Whitman. 1161.
[11] Burduli Irakli et al. 2013. *Constitutional Commentaries – Chapter two, Georgian Citizenship and Basic Human Rights and Freedoms.* Petiti Press. 9.
[12] *Ibid.* 5.

Despite the distinction suggested by Whitman, Francesca Bignami contends that in terms of informational privacy, constitutional protection against governmental intrusion appears to be more robust in Europe than in the U.S.[13] Notions of dignity and free development of personality did indeed fulfill an important role in expansive interpretation of privacy by German and Georgian Constitutional Courts. Had there been a will by the U.S. Supreme Court however, fourth amendment could achieve the same result.[14] This thesis examines and compares domestic Supreme/Constitutional Courts approaches to the problem of abuse of power in conducting electronic surveillance in each jurisdiction and draws the conclusions on its effects on privacy v. security tradeoff.

[13] Bignami, 612.
[14] Gray, 69

1 Electronic Surveillance and Protection of Privacy

In order to establish the limits on governmental interference, it must first be determined what is it that right to privacy protects. According to Daniel Solove, failure to conceptualize privacy may lead to the erosion of its most significant purposes.[15] Constitutional provisions themselves, with the historical and ideological contexts in mind, may provide an important insight into the purposes of the privacy protection, considering the broad and vague language of the Constitution, however Courts are entrusted with the vital task of the interpreting the Constitution. Following chapter will examine constitutional protection of right to privacy in light of the decisions of the Courts in each jurisdiction and discuss their practical consequences for setting the limits on governmental action.

1.1 Protection of Privacy in the U.S.

1.1.1 from trespass doctrine to reasonable expectation of privacy

Not explicitly mentioned in the constitution, right to privacy in the U.S. had developed through the jurisprudence of the Supreme Court as an implicit right in relation to several constitutional provisions. In the context of electronic surveillance, Constitutional protection of privacy stems from the fourth amendment, which guarantees the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[16] It protects "sanctity of the home and confidentiality of communications from undue governmental

[15] Solove, Daniel. 2008. *Understanding Privacy.* Cambridge, Mass.: Harvard University Press. 2.
[16] U.S. Const. amend. IV

interference."[17] Consequently, vindicating the right to privacy in U.S. depends on whether the governmental action at stake can be qualified as a search and seizure.

Right to privacy in U.S. has a negative meaning, securing a person from undue governmental intrusion.[18]According to the American understanding, fourth amendment has a limited application to "certain kinds of governmental intrusion rather than a general recognition of a constitutional "right to privacy."[19] Historically, enactment of the fourth amendment is related to the concept of "general warrant" which was used during colonial period as a blanket authorization of executive officials to conduct searches and seizures without accountability.[20] It was thus designed to constraint "natural tendencies of governments … to expand their reach and control".[21]

Fourth Amendment jurisprudence however, largely frustrates this aim by focusing on technicalities or outdated doctrines. As Daniel Solove points out Americans focus more on the place where the surveillance occurs rather than its problematic effects.[22] The technology had developed in a manner not foreseen by the time fourth amendment was enacted and the ideological commitment to freedom has proven to be of a little help to eliminate governmental inclination to abuse the increased possibilities of information-gathering. Still, Supreme Court had long resisted to stretch the text of the constitution beyond their possible practical meaning to include wiretapping of a telephone within the scope of "search and seizure".[23]

[17] Solove, *Understanding Privacy*, 3.
[18] Jacoby, Nicole. 2007. Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and United States. *Georgia Journal of International & Comparative Law*. 35 (3):435-493. 491.
[19] *Katz v. United States*, 389 U.S. 347 (1967). 350.
[20] Gray, 69.
[21] *Ibid.*
[22] Solove, *Understanding Privacy*, 110.
[23] *Olmstead v. United States* 277 U.S. 438 (1928).

In the case of *Olmstead v. United States*, the U.S. Supreme Court held that wiretapping telephones without actual trespass in the property, did not amount to search and seizure.[24] Justice Brandeis, the co-author of the famous article "the right to privacy" made a strong dissent to the majority opinion, referring to wiretapping as a potential tool for tyranny and oppression and stressing the importance of adapting constitutional provisions designed to guarantee individual protection against abuse of power to a changing world.[25] Despite a harsh criticism however, the Supreme Court affirmed the trespass doctrine in subsequent cases and thus, left wiretapping and other electronic surveillance techniques out of the constitutional realm.[26]

As the instances of wiretapping scandals grew considerably and Congressional attempts to regulate such measures either failed completely or were insufficient to address the problem of abuses, it was the Supreme Court again, who was called for introducing the necessary change.[27] Consequently, In *Berger v. New York*, the Court reiterated that the central purpose of the Fourth Amendment "was to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials" and found that intercepting telephone conversation through electronic devices constituted a "search" within the meaning of the Fourth Amendment.[28]

In the same year, Court declared in its landmark decision of *Katz v. United States* that fourth amendment "protects people, not places." It thus rejected the trespass doctrine and attached decisive importance to what a person "seeks to preserve as private" instead.[29] To clarify the standard established by Katz, Justice Harlan in his concurring opinion elaborated a two-fold criterion of "reasonable expectation of privacy". According the Harlan's test, in order to enjoy

[24] *Ibid.* 465.
[25] *Ibid.* 465.
[26] *Goldman v. United States*, 316 U.S. 129 (1942).
[27] Solove, Daniel J. Rotenberg, Marc. Schwartz, Paul M. 2006. *Privacy, information, and technology*, New York: Aspen Publishers. 83.
[28] *Berger v. New York*, 388 U.S. 41 (1967).
[29] *Katz v. United States*, 389 U.S. 347 (1967).

fourth amendment protection, the person concerned should have a subjective expectation of privacy and the expectation should be considered as "reasonable" in view of the society in general.[30]

By shifting focus from places to people, Katz marked an important development in application of fourth amendment. According to the reasonable expectation test however, fourth amendment protection did not apply to "what a person knowingly exposes to the public" and "to the objects, activities, or statements that he exposes to the "plain view" of outsiders.[31] These limitations have proven to be problematic in subsequent cases.

In *United States v. Knotts* U.S. Supreme Court ruled that tracking a car by a beeper, that Police inserted in the chloroform container, did not amount to a "search" within the meaning of the fourth amendment.[32] According to the Supreme Court, "a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements."[33] Fact that the visual observance of the movement of an automobile is possible from public places has been proven to be decisive in rejecting a claim of any reasonable expectation of privacy.[34] On the other hand, in United States v Karo, also involving installment of a beeper on a container, the movements were tracked in private residence outside the reach of a public eye, which lead the Court to rule that it implicated fourth amendment protection.[35] It follows from these cases that Court reasoning goes along the "firm line at the entrance to the house"[36] and attempt to shift the protection from "places" to the "people" has not been effectively achieved.

[30] *Ibid.* 361.
[31] *Ibid.* 351.
[32] United States v. Knotts, 460 U.S. 276 (1983).
[33] *Ibid.* 277.
[34] *Ibid.*
[35] *United States v Karo*, 468 U.S. 705 (1984).
[36] *Payton v. New York*, 445 U.S. 573 (1980). 590.

1.1.2 Third-Party Doctrine

Another considerable limitation to privacy protection originating from the concept of "reasonable expectation of privacy" is the third-party doctrine developed by the Court in *United States v. Miller.* The case involved collection of customer's financial data from bank records without a knowledge of the affected party.[37] According to the Court, while voluntarily conveying the financial information to the banks, the depositor takes the risk of revealing that information by the bank to the Government. The Court concluded that disclosing the information to a third party absolved any "reasonable expectation of privacy" protected under the fourth amendment.[38]

Few years later, the Court applied the third-party doctrine *Smith v. Maryland* to pen registrars used to record the numbers dialed through a phone.[39] Apart from affirming the third-party doctrine, the Court in *Smith* drew a distinction between content and non-content communications data. Referring back to the *Katz*, that involved the interception of the content of the telephone conversation, court stated that pen registrar only revealed the numbers dialed by a telephone and did not disclose any "communication between the caller and the recipient of the call."[40] The Court thus reached the conclusion that whereas the petitioner's conduct would justify the expectation of keeping the contents of the telephone communication private, no such legitimate expectation existed in relation to the numbers dialed since a reasonable consumer is aware that the phone company keeps the records of such data.[41] Thus, by voluntarily conveying the

[37] *United States v. Miller*, 425 U.S. 435 (1976).
[38] Ibid. 425 U. S. 444
[39] *Smith v. Maryland*, 442 U.S. 735 (1979).
[40] *Ibid*. 742.
[41] *Ibid.* 744.

information to a third party a person, assumed the risk of its disclosure and forfeited the fourth amendment protection.[42]

Comparable factual background in Germany on the other hand, led to a different outcome in Connection Capture opinion of German Constitutional Court, which ruled that constitutional protection of privacy extended to the communications proceedings, such as dialed numbers as well.[43] Similarly, Georgian Constitutional Court has held that dialed phone numbers as well as other kinds of communications proceedings can provide a detailed image of different aspects of personal life and thus, be no less important than the content of the communication itself.[44]

1.1.3 GPS surveillance - United States v. Jones

In a more recent judgment of *United States v. Jones*, The Court did find that attaching a GPS device to the car constitutes a "search" within a fourth amendment.[45] This can barely be considered as a step forward however, bearing in mind that justice Scalia's opinion goes back to the trespass doctrine developed before *Katz* test. Justice Scalia used a textual analysis to conclude that fourth amendment secures not people in general, but people "in their persons, houses, papers, and effects" and it was applicable in this case because the vehicle fell within the meaning of the "effect".[46]

Scalia's reasoning was disapproved by two separate concurring opinions of five justices. In Justice Alito's concurring opinion joined by Justice Ginsburg, Justice Breyer, and Justice Kagan,

[42] *Ibid.* 745.
[43] Schwartz, Paul. M. 2002. German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance, *Hastings Law Journal*, 54, (4): 751-804. 777.
[44] Public defender of Georgia et al. against Georgian Parliament. 2016. Constitutional Court of Georgia 1/1/625, 640. II para 92.
[45] *United States v. Jones, 565 U.S*. 400 (2012).
[46] *Ibid.* II. A.

he criticizes Scalia's application of outdated trespass doctrine which has been replaced by the test of "reasonable expectation".[47] According to Justice Alito, Justice Scalia's highly technical approach neglects the intensity and the effects of the surveillance. Instead, he suggests taking the duration of the measure into consideration while assessing person's "reasonable expectation of privacy".[48]

In Alito's view, a person may not have a reasonable expectation to be free from governmental observance in a single car trip, but such expectation exists when it lasts for a month. In this sense, Alito attempts to shift the focus of the fourth amendment protection to the scope of the information gathered.[49] While the Court has previously refused to take into consideration the "quality or quantity of information obtained" in determining the fourth amendment protection, Alito's opinion marks the direction towards more substantive analysis of the interference.[50]

In a separate concurring opinion Justice Sotomayor went further to suggest the revision of privacy doctrines developed by the Court in view of its primary purposes and necessary adjustments to the technological advancement.[51] She highlighted that current standards did not adequately reflect the reality of a digital age, in which "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane task".[52] According to Sotomayor, entrusting the executive with the unchecked power to deploy "a tool so amenable to

[47] *United States v. Jones*, 565 U.S. 400 (2012), Concurring opinion of Justice Samuel A. Alito, Jr. 957.
[48] *Ibid.*
[49] *Ibid.* 964., Cole, David. 2014. "Preserving the right to privacy in a digital age," in *Surveillance, Counter-terrorism and Comparative Constitutionalism*, eds. Davis, Fergal, McGarrity, Nicola and Williams Abingdon. George. Oxon: Routledge, 101.
[50] *Kyllo v. United States*, 533 U.S. 27 (2001).
[51] *United States v. Jones*, 565 U.S. 400 (2012). Concurring opinion of Justice Sotomayor, 955.
[52] *Ibid.* 957.

misuse" runs counter to the principal goal of fourth amendment to curb arbitrary exercises of police power.[53]

Third-party doctrine developed by the Court in *Miller* and *Smith* excluded a broad scope of personal information from the fourth amendment protection, which was already problematic at the time of the ruling, but even more so in a view of the technological developments that made vast amount of data available to the third parties, and through them – to the government. Refining the concept of privacy in U.S. is thus a crucial step towards preserving the right to privacy in a digital age[54] and the concurring opinions of Supreme Court justices might be seen as a shift towards a new direction.

1.2 Protection of Privacy in Germany – Right to Informational Self-Determination

1.2.1 German Basic Law and the Right to Privacy

Even though the privacy laws have further roots in German history, past abuses and a commitment to personal dignity had significantly influenced the modern concept of right to privacy.[55] Inviolability of human dignity is guaranteed by Article 1 of the Basic Law, whereas Article 2 secures every person "the right to free development of his personality."[56] These two provisions together has been interpreted by Constitutional Court of Germany as the basis for the right to informational self-determination. In addition to dignity and free development of

[53] *Ibid.* 957.
[54] Cole. 108.
[55] Bignami, 687.
[56] Basic Law for Federal Republic of Germany, Article 2 (1)

personality, German Basic law includes separate articles that guarantee "privacy of correspondence, posts and telecommunications" and "inviolability of home".[57]

In order to understand the constitutional protection of privacy in Germany, it is important to look into the specific features of German Constitution. First, the Basic Law allows for limitations of fundamental rights either provided by the constitution itself, by a statute, or by a statute within constitutionally mandated limits. Article 2 for example, allows such limitation if the right of free development of personality "violates rights of others or offends against the constitutional order or the moral law"[58], article 10 permits restrictions pursuant to law,[59] whereas article 13 specifies limits to legislative discretion by specifying certain conditions.[60] If the limitation is not envisaged by the constitution, it can only be restricted when it conflicts with other basic rights, with the exception of human dignity, which cannot be compromised in any event.[61]

Secondly, according to the basic law, restriction of a basic right by a public authority is subject to a judicial review.[62] Furthermore, it recognizes the essence of the right inviolable, which means that limitation is only possible if it does not infringe upon its core.[63] In the context of the right to privacy, German Courts have established a sphere theory, which classifies spheres of personal life according to the level of privacy and recognizes the most intimate sphere of personal life as inviolable.[64]

Lastly, the restriction of basic rights should comply with the principle of rule of law, enunciated in Article 20 (3) of the constitution, which states that "the legislature shall be bound

[57] Basic Law for Federal Republic of Germany, Articles 10 (1) and 13 (1)
[58] Basic Law for Federal Republic of Germany, Article 2 (2)
[59] Basic Law for Federal Republic of Germany, Article 10 (2)
[60] Basic Law for Federal Republic of Germany, Article 13
[61] Jacoby, 458.
[62] Basic Law for Federal Republic of Germany, Article 19, (3)
[63] Basic Law for Federal Republic of Germany, Article 19
[64] Jacoby, 482.

by the constitutional order, the executive and the judiciary by law and justice". In applying this principle, Constitutional Court of Germany has the "principle of proportionality", according to which, the basic right can only be limited for a legitimate aim, by means which are suitable and necessary for its accomplishment. Means will be deemed suitable if no less burdensome alternative could reasonably be expected to achieve the same result.[65] To strike a balance between competing interests the Court takes into consideration the significance of the right infringed, the nature of the intrusion by state and comparable weights of the harm incurred by an individual and the benefit to be achieved by the measure.[66]

In Germany, right to privacy includes negative as well as positive dimension. Thus, apart from being free from governmental intrusion, effects of electronic surveillance measures on dignity and personality rights are also examined.[67] German Constitutional Court has applied dignity-based perspective in its jurisprudence to preserve the values of individual self-determination "in view of modern developments and their accompanying threats to human personality."[68]

1.2.2 Microcensus and Census Act Cases

In Microcensus decision, Court declared that turning a person into a mere object of a state is contrary to the constitutional guarantee of human dignity.[69] According to the Court, Dangers of objectifying a person arises from registering and arranging personal information to create

[65] Jacoby, 460.
[66] Miller, Russell A. 2017. A Pantomime of Privacy: Terrorism and Investigative Powers in German Constitutional Law. *Boston College Law Review*. 58 (5): 1545-1628. 1571.
[67] Jacoby, 436.
[68] Eberle, 1001.
[69] Gerrit, Hornung and Schnabel, Christoph. 2009. Data protection in Germany I: The population census decision and the right to informational self-determination. Computer Law and Security Review: The International Journal of Technology and Practice, 25 (1):84-88. 87.

complete personality profiles that would be accessible to the state.[70] Such profiles enable purposeful linkage of the originally obtained data in order to generate additional information. Thus, when combined together, initially harmless information can turn to a sensitive private data that a person did not intend to disclose.[71]

Having to resolve similar problem of personality profiles, GCC invented a new right to information-self-determination in its landmark decision of Census Act case. Census Act of 1983 required collection of comprehensive information about demographic and social structure of Germany, which, apart from population count, included personal data such as name, address, gender, marital status, religion, occupation, income, education etc.[72] Concerned with the dangers of misuse of this information in view of the growing surveillance and computerization, over one hundred people challenged the constitutionality of the Act.[73]

According to GCC, technological advances since the microsensors decision has enabled more far-reaching intrusion with less effort from the state.[74] Court stressed that collection of comprehensive information carries the risk of creating complete personality profiles trough integrated information systems and automated data processing, which would be available to the state without giving the affected party a chance to control the accuracy or the use of such data.[75] Depriving a person with a possibility to control what kind of personal information is known or disclosed regarding him/herself, can inhibit freedom choice of an individual and personal self-determination.[76] Right to informational self-determination thus, according to the court, is based

[70] *Ibid.* 87.
[71] *Ibid*. 86.
[72] Eberle,1000.
[73] Hornung, Data protection in Germany I: The population census decision and the right to informational self-determination. 85.
[74] Jacoby, 466.
[75] BVerfGE 65, 1. (1983) II, 1 "a".
[76] *Ibid.*

on right to free development of personality under Article 2.1 in conjunction with Article 1.1 of the Basic Law, which, entitles an individuals to control the disclosure and use of their personal data.[77]

By recognizing separate right to informational self-determination, German Constitutional Court confirmed the centrality of human personality in its value-system. According to the Court, apart from an individual right, safeguarding individual self-determination is a prerequisite for a free democratic society based on the freedom of action and self-governance.[78] Such an approach places an individual at the core of the privacy protection not only "to be left alone" but to develop freely in a democratic society, which is in the interests of the community as a whole. [79] At the same time, however, the Court recognized the limits to right to informational self-determination by pointing out, that individuals develop themselves through communication within the social community and even the personal information may reflect social reality that does not belong only to the affected parties. Court thus concluded that tensions between individual and community should be resolved through careful balancing in order to accommodate civic participation and responsibility.[80]

As the technological advancement grew over time, so did the Court's expansive interpretation of the right to privacy. In its judgment on online searching of computers, the Court developed a new facet to right to informational self-determination adapted to the age of information technology. While ruling on the constitutionality of an Act of North Rhine-Westphalia, which allowed Office for the Protection of the Constitution of the State to secretly access information technology systems. GCC developed a new fundamental right to

[77] *Ibid.*
[78] Eberle, 1002.
[79] Eberle, 86.
[80] BVerfGE 65, 1. (1983) "b"

confidentiality and integrity of information technology systems. One aspect of the new right refers to the confidentiality of the personal data created, processed and stored in by the IT system, whereas another aspect requires maintenance of the integrity of the protected information technology against unauthorized use of its "performance, functions and storage contents" by third parties.[81] Bearing in mind the significance of the trust of an individual into the confidentiality and integrity of IT systems for free development of personality, the basis again relied on the "loophole-closing" feature of general right to personality[82] to "counter new types of endangerment" in the context of technological advancement.[83]

The right of informational self-determination has thus become an additional constitutional guarantee for an individual to the extent the other rights did not provide adequate protection of privacy and has been consistently relied upon by the GCC in subsequent cases to curb the excessive surveillance powers of the state.

1.3 Protection of Privacy in Georgia – free development of personality

Structural as well as the foundational principles of the Constitutional protection of piracy in Georgian bears a significant resemblance to the German approach. Even though the Constitutional Courts jurisprudence is much scarcer, its case law demonstrates the direction towards the expansive interpretation of privacy as well as application of rule of law principle trough proportionality analysis. Moreover, similar to Germany, right to privacy under Georgian Constitution also comprises two aspects of guarantees: on one hand, the state has an obligation to

[81] 1 BvR 370/07 (2008) 294.
[82] *Ibid.* 168.
[83] *Ibid.* 169.

ensure the protection of the free development of personality primarily by removing barriers and limitations to the exercise of such right and on the other it has a negative obligation not to allow arbitrary interfere with the right to private life.[84]

Being the youngest among the three jurisdictions, right to privacy guaranteed under Georgian Constituting is the most exhaustive and responsive to the technological developments. According to the paragraph 1 Article 20 "private life, home, personal papers, correspondence, communication by telephone, and by other technical means, including messages received through other technical means are inviolable." In addition to general right to privacy, article 16 of Constitution of Georgia "guarantees free development of personality,"[85] which, according to the Constitutional Court of Georgia, comprises specific aspect of privacy related to personal autonomy.[86]According to the Constitutional Court of Georgia, right to privacy is the expression of human dignity and personal freedom.[87] It has interpreted article 16 of the Georgian Constitution to include general freedom of action and individual self-determination, that provides protection for the aspects of privacy not covered under article 20.[88]

Rather than inventing new fundamental rights under the existing rights system, Constitutional Court of Georgia has developed an expansive, open-ended interpretation of right to free development of personality.[89] While ruling on the constitutionality of surveillance laws in its most recent decision court has listed wide scope of areas under the definition of right to personality, including, among others right to informational self-determination. Court did not

[84] Georgian Young Lawyers Association and Ekaterine Lomtatidze against Parliament of Georgia, Constitutional Court of Georgia N1/3/407. (2007) II, 4.
[85] Constitution of Georgia, Article 16
[86] Georgian Citizens – Alexandre Macharashvili and Davit Sartania against Georgian Parliament and Ministry of Justice, Constitutional Court of Georgia, N 1/2/458, (2009) II, 21.
[87] *Ibid.* II, 2
[88] Alexandre Macharashvili and David Sartania against Parliament of Georgia and Ministry of Justice of Georgia, II, 21.
[89] *Ibid.* II, 4.

however go further to elaborate the content of such right within the meaning of free development of personality.[90] Such definition was given in the context of Article 20 guaranteeing the confidentiality of communications. According to the Court, Article 20 encompasses the right of an individual to express themselves freely without cohesion or self-censorship and in this sense, resonates with the right to informational self-determination and freedom of expression.[91]

Like German Constitutional Court, Georgian Constitutional Court has recognized the general value of privacy protection for the development of a democratic society. The Court has emphasized that Article 16 is of essential importance as its definition creates the borderline between democracy and "police government". Accordingly, failing to strike the proper balance in this sphere could question the stability of democracy itself.[92] While resolving the tensions between private and public interests, legislature should be mindful of enhancing social coexistence while at the same time ensuring personal freedom.[93]

1.4 Conclusion

With a pronounced commitment to centrality of human personality and the rule of law principle, German and Georgian Constitutional have developed an expansive interpretation of privacy recognizing its value for an individual as well as public in general. The U.S. Supreme Court on the other hand, has been reluctant to adapt the demands of privacy protection to the contemporary technical developments. It treats privacy as an "on/off affair"[94] meaning that Certain government actions fall outside the scope of the fourth amendment regardless the amount

[90] Public defender of Georgia et al. against Georgian Parliament, II, 6.
[91] *Ibid.* II, 24.
[92] Georgian Young Lawyers Association and Ekaterine Lomtatidze against Parliament of Georgia II, 4.
[93] *Ibid.* II, 7.
[94] Cole, 10.

and importance of the obtained information and its effects to the privacy of an individual. It has thus granted far broader leeway to the political branches in choosing the scope and means of electronic surveillance than the European Counterparts.[95] The Supreme Court thus, opened up loopholes to privacy protection German and Georgian Courts have tried to close.

[95] Schwartz, Paul M. 2011. Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the States, and New Technology, William & Mary Law Review., 53 (2): p351-387. 382

2 Surveillance and National Security

2.1 Judicial warrant requirement in national security cases in the U.S.

2.1.1 Executive-Judicial Tension

Historically, in the U.S. executive-judicial tension over national security matters tended to arise during the times of unrest, which was used as a justification for expansion of the executive powers against foreign threats. Warrantless surveillances by President Nixon and President Bush follow a similar pattern of events. The raise of domestic protests on one hand and terrorist attacks on the other, triggered the appeal over the inherent constitutional powers to defend the nation.[96]

In *Katz*, the Supreme Court recognized the prior judicial approval as a precondition for wiretapping. According to the court, limits on governmental action should be placed by a neutral magistrate who will deal with the case with detached scrutiny based on the assessment of a probable cause.[97] Judicial warrant requirement for wiretapping established by *Katz* was however limited to ordinary crimes only, leaving the standards for national security cases open to question.[98]

Concurring justices in *Katz* had presented opposing views regarding the warrant requirement in national security cases. Recalling a long-standing practice of wiretapping authorizations by successive Presidents, Justice White endorsed the exemption from judicial warrant requirement

[96] Bloom, Robert. Dunn, William J. 2006. The Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment, *William & Mary Bill of Rights Journal*. 15: 147-202.148.
[97] *Katz v. United States*, 356- 359.
[98] *Ibid.* footnote 23.

when national security was at stake.[99] Justice Douglas, joined by Justice Brennan on the other hand, condemned such exemption, considering it to be a green light for the executive branch to use unwarranted electronic surveillance for the cases it labeled as "national security" matter.[100]

While enacting an Omnibus Crime Control and Safe Streets Act of 1968 to comply with *Katz* and *Berger,* congress exempted the national security cases from the warrant requirement.[101] Section 3 of 2511 of title III provided as follows:

> "nothing contained in this chapter [shall] limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government."[102]

The above exception was used by the President Nixon to circumvent warrant requirement and statutory restrictions for surveilling domestic dissidents and radicals.[103] Nixon initiated the intelligence-gathering program collecting the data of over 100,000 Americans in the name of warding off the threats to national security.[104] Nixon's surveillance program was based on the justification that domestic protests against the backdrop of the Vietnam War were supported by foreign power and thus fell under his constitutional competences of war and foreign policy powers.[105] Massive abuses were uncovered as a result of the investigations carried out by Congressional Committee headed by Senator Church. Committee report expressed concerns

[99] *Ibid.* 389.
[100] *Ibid.* 389.
[101] Solove, *Privacy, information, and technology*, 85.
[102] Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2511 (3)
[103] Solove, *Privacy, information, and technology*, 85.
[104] Zeugmann, Cora. (2008) Cora The Trade-Off between Civil Liberties and Security in the United States and Germany after 9/11/01, Hamburg: Diplomica Verlag. 41.
[105] Bloom, 149.

about unrestrained, indiscriminate intelligence-gathering, that has been launched and continued without any review upon its impact "on the constitutional rights of Americans."[106]

2.1.2 United States v. United States District Court

The Supreme Court addressed the issue of national security exemption in *United States v. United States District Court*, the so-called Keith case. The controversy in *United States v. United States District Court* concerned the affidavit issued by the Attorney General to authorize warrantless surveillance in order to prevent domestic organizations from attacking and subverting the "existing structure of the Government."[107] While the Court found no evidence of involvement of foreign power, it limited its inquiry to the question of whether using electronic surveillance measures without prior judicial approval to prevent threats to national security would be compatible to the fourth amendment.[108]

The U.S. Government contended that national security exemption under Article 2511 (3) of the title III authorized the President to resort to electronic surveillance through Attorney General in order to protect the state against subversive activities at domestic level.[109] By rejecting the argument that domestic surveillance fell under the Constitutional powers of the President to "preserve, protect and defend the Constitution of United states", Court stipulated that Article 2511 (3) was aimed at excluding limitations on existing Presidential powers, not to confer a new one.[110]

The Court based its inquiry on "reasonableness" requirement of fourth amendment. By stating that the fourth amendment was not absolute, Court engaged in balancing competing interests

[106] Zeugmann, 41.
[107] *United States v. United States Dist. Ct.*, 407 U.S. 297 (1972). 300.
[108] *Ibid.* 319.
[109] *Ibid.* 303.
[110] *Ibid.*

between domestic security on one hand and privacy and freedom of speech as an essential prerequisite for free society on the other.[111] According to the Court, even though the "reasonableness" requirement under the fourth amendment relates to the search and seizure in general and not to the issuance of a search warrant, warrant clause represents a more specific condition of reasonableness which should not be overlooked.[112] The Court stressed that the involvement of a "neutral and detached magistrate" was at the core of the warrant requirement, which is further supplemented by the standard of "probable cause" to draw the boundaries for the executive action.[113]

Citing the Justice Douglas's concurring opinion in Katz, Court reiterated that the executive branch is not neutral and detached authority in matters concerning domestic security, but rather interested in preventing threats and prosecuting criminals.[114] Consequently, decision on deploying constitutionally sensitive means for fulfilling their duties should not be left to their sole discretion.[115] Prior Judicial oversight is thus a necessary check to the executive discretion in accordance to the principle of separation of powers and the exceptions to this requirement should have be interpreted narrowly.[116]

Court rejected government's argument that the complexities of domestic security cases and the risk of compromising necessary secrecy of intelligence-gathering renders the Courts ill-suited to fulfill the oversight function. It also did not agree that the burden of prior judicial approval would significantly weaken the surveillance powers of the government.[117] In view of the risks of using "inherent vagueness of the domestic security concept, the necessarily broad and continuing

[111] *Ibid.* 314.
[112] *Ibid.* 315.
[113] *Ibid.* 315.
[114] *Ibid.* 317.
[115] *Ibid.*
[116] *Ibid.* 315.
[117] *Ibid.* 321.

nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent," Court was not convinced that "complete exemption of domestic security surveillance from prior judicial scrutiny" was justified.[118]

At the same time, Court noted that declaring warrantless surveillance in domestic security cases unconstitutional did not mean that it should necessarily be treated in the same way as an ordinary crime under title III, thus, permitting less stringent standards to be applied.[119] Less precise focus of domestic surveillance would be justified by nature of intelligence gathering, which is often preventive, directed towards future threats, and requires long-range information collection from various sources.[120]

Considering the long-standing practice of warrantless presidential authorizations for domestic surveillance, Supreme Court in *Keith* made an important determination in upholding the judicial warrant requirement in cases involving internal security. Court however, pointed out that its decision should not be understood to address the cases involving foreign powers and their agents.[121] Given that the question has not been raised before the Court ever since, the issue remains under the congressional regulation.

2.2 National Security exemption in Germany

2.2.1 G10 amendment

Whereas in the U.S. the distinction between domestic and foreign intelligence gathering was brought about by a Supreme Court to curb massive executive abuses, Germany introduced differentiated standards with regard to ordinary crimes and those affecting the "free democratic

[118] *Ibid.* 320.
[119] *Ibid.* 322.
[120] *Ibid.*
[121] *Ibid.*

basic order or the existence or security of the Federation or of a Land" by a constitutional amendment.[122] The change was a part of the anti-terror measures against emerging violent radical leftist movements and student protests across the Country in 1969.[123]

As a result, paragraph 2 of the article 10, provided that judicial review of restrictions to the privacy of correspondence, posts and telecommunications could be replaced "by a review of the case by agencies and auxiliary agencies appointed by the legislature" if the national security was at stake. Additionally, in such cases, the state could be exempted from obligation to notify the affected party about the interference.[124] Exception was reflected in Article 19 (4) as well, which excluded the right to have a recourse to court in cases covered by second sentence of paragraph (2) of Article 10.[125]

Amendment was followed by enactment of so called G10 statute, regulating surveillance procedures for national security cases. Unlike in ordinary criminal cases, statute exempted surveillance measures for national security purposes from judicial pre-approval and prohibited notification of surveillance targets after such measures. According to the statute, authorization to wiretap could be requested by agencies entrusted with counterintelligence matters and warrants could be issued by Minister of the Interior and Minister of Defense in domestic and strategic (external) surveillance respectively.[126]

Oversight of minister's decisions was carried out by two bodies. Parliamentary board (G10 board) comprised of five members representing cross-section of political parties reviewed semi-annual reports presented by each minister. G10 board was also responsible for appointing a

[122] Basic Law for Federal Republic of Germany, Article 10
[123] Miller, Russell A. 2010. Balancing Security and Liberty in Germany. *Journal of National Security Law & Policy.* 4, (2): 369-396. 375.
[124] Basic Law for Federal Republic of Germany, Article 10 (2)
[125] Basic Law for Federal Republic of Germany, Article 19 (4)
[126] Barnum, David G, 2016. Judicial Oversight of Interception of Communications in the United Kingdom: An Historical and Comparative Analysis null. *Georgia Journal of International and Comparative Law*. 44, (2): 237-304. 254.

three-member "G10 Commission", a body to which each Minister had to submit monthly account on the orders issued. Moreover, Commission was also vested with the power to review wiretap orders and receive applications from persons who believed to be targets of surveillance. Finally, Commission could request termination of surveillance it considered illegal or unnecessary." [127]

Group of German citizens, including a state prosecutor Gerhard Klass, challenged the constitutionality of G10 statute and the amendment.[128] Constitutional Court upheld the constitutionality of G10 statute, largely relying to a concept of "defensive democracy", as an underlying principle of German Constitution. According to the concept of "Defensive democracy" "enemies of the Constitution must not be allowed to endanger, impair or destroy the existence of the state while claiming protection of rights granted by basic law."[129] The Court thus, concluded that the constitutional organs entrusted with the power to protect the constitution should not be deprived of necessary means for the execution of their functions.[130]

Apart from emphasis on "defensive democracy", Court stressed that in view of its whole context, the Basic Law placed an individual not merely as an isolated entity but as a part of a community. Consequently, the absence of notification requirement to the target of surveillance in national security cases could be justified as a necessary burden to a citizen for the sake of protecting stability of the State and the free democratic order.[131]

While stating that surveillance measures required oversight in order to prevent "the arbitrariness of the administrators", court was satisfied that the oversight of non-judicial body

[127] *Ibid.*
[128] Kommers, Donald P. 1997. *The constitutional jurisprudence of the Federal Republic of Germany*. Durham: Duke University Press. 228.
[129] Schwartz, German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance. 774.
[130] Kommers, 229.
[131] Schwartz, "German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance", 775.

(G10 Commission) comprised of independent members ensured an efficient "material and procedural control" thereto.[132] Court however, found prohibition of notification of affected person under all circumstances, regardless of whether such notification would endanger the goal of the restriction to be unconstitutional in light of principle of proportionality.[133]

2.2.2 Strategic Surveillance Case

Since the domestic upheaval during 70ies and 80ies, expanding the secret surveillance measures in Germany came into agenda during the relatively peaceful period with a new concern related to international terrorism and organized crime.[134] 1994 amendments increased the powers of Federal Intelligence Service to carry out international telecommunications surveillance for broader scope of offences without the need to establish a "probable cause" if these crimes could be linked to a threat of attack on Germany.[135] Strategic surveillance differed from individual investigation as it deployed a new technologies to intercept communications data to and from Germany using specific "search terms".[136] Amendment further removed barriers on data-sharing between intelligence and police agencies allowing the use of intelligence information in criminal prosecutions.[137]

GCC first recognized that Article 10 guarantees applied to the communications that did not entirely fall within national borders, given that surveillance was conducted from within the

[132] *Ibid.*
[133] *Ibid.* 776.
[134] Miller, Balancing Security and Liberty in Germany. 380.
[135] Jacoby, 468.
[136] Schwartz, German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance. 779.
[137] Miller, Balancing Security and Liberty in Germany. 381.

Germany and at least part of the communication started or ended in Germany.[138] While referring to the Census act case and the right to informational self-determination as an individual as well as societal value, GCC nevertheless considered governmental interest in detecting and responding to the threats to Germany as "a high-ranking public interest" that could justify resorting to the strategic telecommunications surveillance.[139] Court thus upheld the major part of the statute, striking only few provisions concerning information-exchange and notification requirement.

While allowing the surveillance without probable cause, Court concentrated on improving safeguards with regard to dissemination of collected information.[140] In accordance to the principle of proportionality, data transfer would be permissible if it revealed the commission of serious offences.[141] Furthermore, considering the automatic deletion of the collected data insufficient for preventing its misuse and the Court required affected parties to be notified after the surveillance measures, save the exceptional cases when it would jeopardize an ongoing investigation.[142] Finally, the Court demanded the improved parliamentary oversight as an additional check to ensure that the entire procedure of data collection and assessment meet the prescribed standards.[143]

[138] Schwartz, German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance. 780.
[139] Miller, Balancing Security and Liberty in Germany. 381.
[140] Jacoby, 469.
[141]Schwartz, German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance. 782.
[142] Jacoby, 469.
[143] Ibid. 470.

2.3 Comparing American and German approaches

The demand for more expansive executive powers in cases involving national security matters came in the forefront of the constitutional debate during a time of domestic upheavals in both the U.S. and Germany. The Courts in both Courtiers have approved the establishment of differing standards for ordinary crimes and those involving national security interests. In essence, both courts showed the deference to the political organs endorsing more lenient standards for the cases involving national security matters.

While in U.S. dividing line of fourth amendment protection lay between its Citizens and foreigners, German Court pronounced the Basic rights to be applicable to any communication that initiated or ended within the German territory. This, on one had means that German citizens can be subjected to the surveillance according to the lesser standard and on the other hand foreign citizens are protected as well.

Conversely, protection of U.S. citizens is higher in the U.S. as any surveillance falling under the scope of fourth amendment would require a judicial warrant, while foreigners do not enjoy constitutional protection at all. As demonstrated by the subsequent statutory developments in the U.S. however, distinction between foreign and domestic threats have gradually faded away by the spillover effects of the broad provisions, allowing incidental surveillance of the U.S. citizens.

Even though the German Constitutional Court upheld the basic features of the new laws, it has still carefully scrutinized each provision and evaluated the safeguards in accordance with the principle of proportionality a stage where most of the cases in U.S. would not reach due to the Supreme Court's restrictive interpretation on the scope of the fourth amendment and its strict standing requirement.

2.4 Judicial warrant requirement in Georgia

In Georgia, on the other hand, no comparable historical events have occurred since the enactment of the new constitution and the threat of international terrorism is more distant than in U.S. and Germany. Being in the transitional period, with the new-born democratic institutions and insufficient privacy guarantees however, warrantless surveillances has been a systematic governmental practice.[144] Major movements towards curbing the executive excesses was prompted by the dissemination of illegal recordings through social network in 2012, just before the Parliamentary Elections.[145] Up to 29, 000 conversations of opposition party members, journalists, and civil society activists have been recorded for political purposes around the period of 2003-2012 by Ministry of Defense's Military Police, Ministry of Internal Affairs and Presidential Security Office.[146] Revelations were followed by a campaign organized by civil society representatives called "it concerns you – they are still listening", urging legislature to enact amendments to covert surveillance laws.

Having explicit judicial warrant requirement in the Constitution for any intrusion to the right to privacy,[147] Constitutional Court of Georgia has not distinguished between the ordinary crimes and national security cases in this regard. In its judgments, it has strictly required judicial warrant as an essential prerequisite for secret surveillance measures regardless of its aims. According to the Court, prior approval by a Court, as a neutral and detached authority, serves to avoid governmental abuses and is especially important in case of covert actions.[148] From a hindsight,

[144] Hammarberg, Thomas. Georgia in transition. Report on the human rights dimension: background, steps taken and remaining challenges Assessment and recommendations, 2013, 24. http://eeas.europa.eu/archives/delegations/georgia/documents/human_rights_2012/20130920_report_en.pdf;
[145] Institute for Development of Freedom of Information, "Regulating Secret Surveillance in Georgia: 2013-2015. www.idfi.ge, May 2015. https://idfi.ge/public/upload/surveillance/Surveillance-final-28-03-2016.pdf, 3.
[146] Hammarberg, 25.
[147] Constitution of Georgia Article 20 (1)
[148] Georgian Young Lawyers Association and Ekaterine Lomtatidze against Parliament of Georgia, II, 24.

this could give an impression that Georgian system recognizes the highest standard of privacy protection. Warrant requirement alone however, did not prove to be sufficient for the prevention of abuses, which can arise in other "creative" ways and thus, a complex system of guarantees is required to ensure that the rule of law does not "slip away through loopholes in individual provisions." [149]

[149] 1 BvR 1215/07. (2013) 157

3 Separation of Police and Intelligence

General difference between police and intelligence agencies lies in their repressive and preventive functions respectively. Police is charged with the law enforcement, largely focusing on the crimes already committed, intelligence services gather and analyze information to prevent future threats.[150] For this reason, data mining has become a main tool for intelligence operations, involving information collection and its subsequent processing with the aim to develop patterns of suspicious behaviors, and profiles that would enable prediction of the upcoming attacks.[151] The rules governing the access and use of the private data by the state authority has thus become the main concern for the effective protection of privacy rights in a contemporary world.

Given the different functions and consequently the thresholds for interference into privacy rights by law-enforcement and intelligence authorities, institutional and informational separation is an important precondition for preventing abuse of power. Even though currently all three jurisdictions have a separated police and intelligence agencies, in view of the overlapping competences[152] and vast cooperation and information-sharing capacities the lines between police and intelligence have been blurred. [153]

[150] Solove, Daniel J. 2008. Data Mining and the Security-Liberty Debate, *University of Chicago Law Review*, 75 (1): 343-362, 343

[151] *Ibid.*

[152] Schwartz, Paul M. 2017. "Systematic Government Access to Private-Sector Data in Germany," in Bulk Collection: Systematic Government Access to Private-Sector Data, Oxford University Press,. 78.

[153] Putter, Norbet The Federal Republic's security services from the Cold War of the "new security architecture", *Statewatch Journal,* 19 (4) 1. http://www.statewatch.org/analyses/no-102-germany-security-services.pdf

3.1 "FISA Wall" in the U.S.

In the U.S. FBI carries out the double-function of domestic intelligence and law-enforcement, whereas foreign intelligence function is undertaken by the National Security Agency.[154] Following the *Keith* Judgment and the report of the Church Committee, Congress enacted a Foreign Intelligence Surveillance Act (FISA) of 1978, creating a specialized court with an exclusive jurisdiction to review the requests for surveillance in foreign intelligence operations.[155] Drawing a distinction between investigations of ordinary crimes and those involving national security issues, FISA established a less rigorous standards for obtaining the warrant for surveilling "a foreign power or an agent of a foreign power".[156] In contrast with the title III requirement, "probable cause" for issuance of a warrant related not to the specific crime but to the belief that a target is a "a foreign power or an agent of a foreign power".[157]

So-called "FISA wall" ensuring the separation between criminal and foreign intelligence investigations and the limited cooperation and information-exchange among corresponding agencies has however "disappeared" since 9/ 11.[158] 9/11 attacks in America has triggered another wave of security legislation directed to extend the executive discretion in preventing the threats to the nation. Enacted shortly after the attacks, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (PATRIOT Act)

[154] Bignami, 621.
[155] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §1803, Sec. 103
[156] Zeugmann, 42.
[157] Barnum, David G. 2006. Warrantless electronic surveillance in national security cases: lessons from America, European Human Rights Law Review 5: 514-540, 529.
[158] Casagran, Cristina Blasi. 2017. "Surveillance in the European Union," in The Cambridge handbook of surveillance law, eds. Gray, David and Henderson, Stephen E. Cambridge University Press; 653.

enabled FISA applications for criminal investigations if "significant" but not necessarily the sole or a primary purpose was to obtain foreign intelligence information.[159]

Even the relaxed standards of Patriot Act however, did not compel the Bush Administration to confine its surveillance within the statutory framework. Bearing a striking similarity with Watergate scandal, Bush lunched warrantless surveillance programs involving an "unprecedented collection of information concerning U.S. persons".[160] Relying upon the inherent war powers and the Congressional authorization under the Authorization for Use of Military Force (AUMF), Bush administration contended that the FISA framework did not apply.[161] Even though the arguments were clearly unfounded, the challenge brought by the ACLU against NSA had been dismissed by the Supreme Court on the basis of lack of standing as the plaintiffs could not demonstrate the concrete harm.[162]

Despite this massive excesses, Congress has been more willing to broaden rather than limit the executive authority.[163] Legalizing the warrantless surveillance programs, 2008 amendments in FISA further removed the barriers for obtaining FISA warrant and enabled blanket authorizations without the need to indicate individual targets as long as it is reasonably believed that the procedure would only address foreigners abroad.[164] This broad language and relaxed standards increased the likelihood of incidental collection of information on U.S. persons and thus, eroded the distinction between foreign powers and U.S. citizens, consequently, circumventing the warrant requirement under the fourth amendment. What is more, it permitted

[159] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001; Public Law 107–56; 115 STAT. 272 §702.
[160] Levinson -Waldman, Rachel 2017. "NSA Surveillance in the War on Terror," in The Cambridge handbook of surveillance law, eds. Gray, David, Henderson, Stephen E. Cambridge University Press. 8.
[161] Bloom, 179.
[162] Levinson-Waldman, 33.
[163] Schwartz, Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the States, and *New Technology*. 382
[164] Fiss, Owen, 2014. "Warrantless wiretapping in the United States" in *Surveillance, Counter-terrorism and Comparative Constitutionalism*, George. Oxon: Routledge. 222.

an incidental information on U.S. citizens collected under the authorization of FISA, to be accessed by FBI without any foreign intelligence purpose.[165]

Only after another scandal surrounding NSA bulk collection of logs of domestic phone calls of U.S. persons modest reforms in FISC procedures and relatively increased safeguards have been introduced by Congress trough USA Freedom Act.[166] The hopes for the better privacy standards however have again been frustrated by renewal of the Section 702, allowing incidental collection of the communications of U.S. citizens.[167]

3.2 Separation Rule in Germany

Mindful of the historical experience of centrally organized police force during the third-Reich, Germany recognized a fundamental rule of organizational and institutional separation of police and intelligence services after World War II, which was aimed at reducing the "political danger" of intelligence services.[168] Police powers under the German law at the federal level fall within the competence of federal police (BKA), whereas intelligence-gathering function is divided between two bodies – federal intelligence service (BND) being responsible for foreign intelligence activities and Federal Office for the Protection of the Constitution – for the domestic one.[169]

Apart from the institutional separation, according to principle of informational separation of powers established by the GCC in its Census decision, state is not to be deemed as a single entity but a composition of multiple data processors, each needing a separate statutory authorization for

[165] Levinson- Waldman, 25.
[166] *Ibid.* 28.
[167] The New York Times, House Extends Surveillance Law, Rejecting New Privacy Safeguards, last modified in Jan. 11, 2018 https://www.nytimes.com/2018/01/11/us/politics/fisa-surveillance-congress-trump.html
[168] Putter, 1., Schwartz, Systematic Government Access to Private-Sector Data in Germany. 72.
[169] *Ibid.* 78.

access and the use of data.[170] This principle is linked to the requirement of purpose limitation and proportionality, according to which, no more data should be processed than absolutely necessary for the specified purpose that meets the standard of clarity and certainty.[171]

The aim of the principle of purpose-limitation is to prevent the transfer of information from agencies subject to the more relaxed standards to those to whom stricter standards apply.[172] To that end, the court distinguishes between the tasks of intelligence and police authorities. Intelligence agencies had vast information-gathering powers due to their limited tasks of "providing early political information" about future threats. Police on the other hand is in charge of crime prevention and repressive measures, concentrating on a situation-specific tasks.[173] Thresholds for interference are accordingly different, broader and less detailed with regard to intelligence data collection as opposed to the narrowly defined powers of Law enforcement.[174] In exceptional circumstances however, where police is endowed with the authority to gather data without specific cause, the Court calls for a need for a particular justification and heightened constitutional requirements.[175]

Principle of specificity derives from the constitutional requirement that the fundamental right can only be restricted by legislation which is sufficiently clear and foreseeable. Legal provision infringing upon a fundamental right should be designed in a way that gives the executive clear guidelines and limits their actions. It should further be predictable enough to enable individuals challenge government action and the Courts to conduct effective Supervision.[176] According to

[170] Hornung. Data protection in Germany I: The population census decision and the right to informational self-determination. 87.
[171] *Ibid.* 87
[172] 1 BvR 1215/07, (2013) 114.
[173] *Ibid.* 118-120.
[174] *Ibid.*
[175] *Ibid.* 120.
[176] *Ibid.* 141.

the GCC Because of the lack of transparency and judicial supervision, requirement of specificity especially rigorous in data privacy law.[177]

3.3 Jurisprudence of German Constitutional Court on Governmental Data Mining

3.3.1 "Anti-terrorism Package" in the aftermath of 9/11

In the aftermath of 9/11 aware of the fact that part of the attacks had been planned from a German territory, Parliament adopted two "anti-terrorism packages" to address potential threats to security.[178] Second "anti-terrorism package" included the expansion of competences of the intelligence authorities to provide them with improved tools to eliminate "dangerous breeding ground for growing terrorism."[179] It enabled police and intelligence agencies to gather information from various financial institutions, postal and telecommunications services and aviation and provided for subsequent exchange of information among them.[180]

Unlike the "Hands-off" approach of U.S. Supreme Court, German Constitutional Court has played an important role in establishing constitutional standards addressing new challenges in the age of big data.[181] The Court has scrutinized security legislation through the proportionality analysis, national security being only one among the many other competing interests such as

[177] *Ibid.*157.
[178] Zoller, Verena, 2004. Liberty dies by inches: German counter terrorism measures and human rights. *German Law Journal*. 5 (5): 469-494. 470.
[179] Rau, Markus. 2004. "Country Report on Germany," in Terrorism as a challenge for national and international law: security versus liberty? Eds. Walter, Christian, Voneky, Silja, Roben, Volker, Schorkoph, Frank. Berlin: Springer. 328.
[180] Zoller, 486.
[181] Schwartz, Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the States, and New Technology. 377.

dignity, privacy and informational self-determination.[182] While recognizing that the investigative measures should be attuned with the increased use of technology by extremists and terrorist groups for planning and committing criminal offences, [183] the Court has focused on developing system of safeguards that would effectively prevent abuse of power.

3.3.2 Data Mining Case

Subsequent to the enactment of "anti-terrorism packages" government launched an extensive data-mining program involving indiscriminate collection of information from private and public institutions in order to create profiles trough data-processing technology that would match the characteristics of so called "sleepers".[184] Such a pattern-based search was for preventive purposes and contrasted with the repressive screening which required "sufficient factual indications to show that a criminal offense of significant importance has been committed".[185] Information on 5.2 million persons have been incorporated in a single database within Federal Criminal Police, program however did to produce any result and the information was finally erased.[186]

The case reached the Constitutional Court, which imposed substantial limits to the use of data-screening technologies. While recognizing the fight against terrorism as a high-ranking constitutional value, the Court considered the infringement of right to informational self-

[182] Miller, Balancing Security and Liberty in Germany. 371.
[183] *Ibid.*
[184] *Ibid.* 386.
[185] Schwartz, 382.
[186] Schwartz, Systematic Government Access to Private-Sector Data in Germany. 69.

determination to be especially grave as such programs could result in a creation of extensively revealing personality profiles.[187]

Mindful of heightened sensitivity towards the security issues in the aftermath of earth-shattering attacks, the Court articulated that the pursuit of the fundamental aim of ensuring security should be subordinated to the principle of rule of law:

> "The Constitution demands that the lawmaker strike a reasonable balance between freedom and security. At its core this mandate excludes the pursuit of absolute security, which is impossible in any case and, even If it were not, could only be achieved at the price of repealing freedom. The Basic Law also limits the state's more concrete efforts to maximize security. The trappings of the rule of law must be observed, in particular, the prohibition of disproportionate infringements upon basic rights. This is a right of protection against the state."[188]

According to the principle of proportionality, preventive action would only be justified upon showing the "concrete danger" to the security of the country, an individual state, or the life of a citizen".[189] A concrete damage would exist in "a state of affairs, under which in the actual case there is a sufficient probability of a damage ... in the near future". Lasting threat would also justify data screening, general threats would not suffice however, as "concrete danger" required a proof of actual preparations for an attack.[190] Nevertheless, the Court did not consider the data screening unconstitutional, constitutionally permissible interpretation of the statute was possible by reading the requirement of "concrete danger" in a term "necessary for the individual case."[191]

3.3.3 Data retention Case

Few years after, Court was called again to rule on the constitutionality of the amendments to Code of Criminal Procedure and Telecommunications Act implementing EU Directive on data

[187] Miller, Balancing Security and Liberty in Germany, 386.
[188] Miller, Balancing Security and Liberty in Germany, 387.
[189] Schwartz, Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, 364.
[190] Ibid. 373
[191] Ibid. 374

retention. Amendments envisaged the obligation of telecommunications service providers to store communications traffic data for six months and its subsequent access and use by the state authorities. As is previously ruled in Connection Capture opinion, protection of basic rights extended not only to the content but also to the process of the communication as well, such as "when and how often telecommunications traffic occurred or was attempted between what persons or telecommunications equipment"[192] Court emphasized that not only initial access, but each subsequent processing and the use of data obtained constitutes a separate encroachment of Article 10.1 of the Basic Law.[193] Thus, the use of data for a different purpose would require an independent statutory authorization.[194]

Given that such storage was not connected to any specific culpable conduct or even an abstract danger, the Court considered its range to be the broadest to date.[195] Furthermore, since the storage and use of communications data is not noticeable by an affected party, Court was particularly concerned with the effects "diffusively threatening feeling of being watched" could have on exercise of fundamental rights.[196] Interestingly, Court recognized the prohibition of total recording and registration of the exercise of freedom of its citizens as part of the Constitutional identity of Germany.[197] Rather than finding the precautionary storage of the traffic data unconstitutional per se the Court focused on the conditions of its implementation. The Court laid down four types of guarantees for preventing abuse, purpose limitation, data security, transparency and legal protection against misuse.[198]

[192] 1 BvR 256/08, (2010) 189.
[193] *Ibid.* 190.
[194] *Ibid.* 236.
[195] *Ibid.* 210.
[196] *Ibid.* 212.
[197] *Ibid.* 218.
[198] *Ibid.* 220.

Firstly, to assess the compliance with the purpose-limitation, the Court scrutinized whether or not the requirements for the use of data and its extent were sufficiently narrowly defined to relate to a specific area in a foreseeable manner.[199] Creation of data pools without prior purpose, leaving its use upon the discretion of state agencies would run counter to this requirement.[200] Retrieval of the telecommunications traffic data for preventive purposes would require an "actual evidence of a concrete danger to the life, limb or freedom of a person, to the existence or the security of the Federation or of a Land or to ward off a danger to public safety".[201] The Court further clarified the concept of "concrete danger" and relaxed its previously established standard of probability of occurrence in "near future" to the one that is foreseeable, provided that "particular facts indicate the threat of a danger to a legal interest of paramount importance."[202] Additionally, the Court demanded the measure be limited to the specific target who are "likely to cause the damage".[203] Further safeguards comprised the deletion of irrelevant data, destruction of data that already served its purpose and keeping records to that end.[204]

Secondly, Court recognized the obligation of the legislature to lay down especially high security standards for storage, transmission and deletion of the data in a well-defined manner and with the adequate supervisory mechanisms and periodic reviews.[205] In order to fulfill the requirement of effective security guarantees, the Court suggested specific measures such as separate storage, sophisticated encryption, a secured access regime and revision-proof recording

[199] *Ibid.* 226.
[200] *Ibid.*
[201] *Ibid.* 231.
[202] *Ibid.*
[203] *Ibid.*
[204] *Ibid.* 235
[205] *Ibid.* 225.

could be adopted.[206] To ensure the adherence to these rules, monitoring requirement by data protection officer and balanced system of sanctions should have also be put in place.[207]

Thirdly, the Court stated that in order to ensure transparency, data should be open "as far as possible" to counter the sense of insecurity resulting from the ignorance as to what is known to the state authorities and a feeling of "being permanently monitored".[208] Additionally, requirement of transparency was aimed at providing the possibility to challenge the unlawful official use of the data or require deletion, correction or legal redress.[209] The duty to notify affected parties should have recognized at least subsequently, unless "otherwise the purpose of the investigation served by the retrieval of data would be frustrated". Such exemption would require a judicial decision to that effect.[210]

Finally, the Court demanded the guarantee of effective legal protection and system of sanctions. In case of intelligence services a prior authorization of data-collection by parliamentary oversight body would be required.[211] With regard to the supervision, the Court attached particular importance to the fact that the communications data is stored by telecommunications service providers in a dispersed manner and is only made available to the public authorities indirectly, for restricted purposes.[212] According to the Court, such decision-making structure involving numerous actors would serve the purpose of mutual supervision.[213]

Applying in a case before it, the Court held that since the provisions on data security, on the purposes and the transparency of the use of data and on legal protection failed to meet

[206] *Ibid.* 224.
[207] *Ibid.* 225.
[208] *Ibid.* 242.
[209] *Ibid.*
[210] *Ibid.* 243.
[211] *Ibid.* 248.
[212] *Ibid.* 214.
[213] *Ibid.* 250.

constitutional requirements, the storage obligation as a whole lacked the sufficient justification and was therefore, unconstitutional.[214]

3.3.4 Counter-terrorism database Case

Creation of a "joint, standardized and centralized counter-terrorism database" involving information-sharing between all law-enforcement and intelligence agencies was another big shift towards extensive cooperation as opposed to separation in Germany.[215] The database founding Act has been challenged before the Constitutional Court. Applying proportionality analysis in a standardized manner, the Court held the creating a database with the purpose of investigating and combating international terrorism was compatible with the right to informational self-determination.[216] The Court required however, more detailed structuring of the database and clear and adequate legal limitations, including effective supervision of its use.[217]

According to the Court, transfer of information among the police and intelligence agencies would only be permissible in exceptional circumstances.[218] It acknowledged however, that allowing an "expedient exchange of findings"[219] among the agencies charged with Counter-terrorism measures would significantly improve their tasks. Thus, the Court found it acceptable that the transfer of the data obtained under less stringent standards for intelligence-gathering for operational functions of the law-enforcement could be allowed in emergencies to protect from specific threats.[220]

[214] *Ibid.* 292.
[215] Miller, A Pantomime of Privacy: Terrorism and Investigative Powers in German Constitutional Law, 1555.
[216] 1 BvR 1215/07, (2013) 105.
[217] *Ibid.* 110.
[218] *Ibid.* 125.
[219] *Ibid.* 131.
[220] *Ibid.* 124.

The database distinguished between "open" and "concealed storage" according to which, information kept in "open storage" would be revealed to the inquiring authority in case of a match, whereas the information kept in "concealed storage" would not. Such an inquiry however would be reported to the agency having stored the data in "concealed storage", which would check the legal basis to decide whether or not to share the information.[221] Thus, apart from the emergencies the data in "concealed storage" could only be used indirectly subsequent to a successful match, which was deemed to be constitutionally permissible.[222] Criteria-based search that provided direct access to the "open storage", was however, considered to be unconstitutional as it allowed retrieval of personal data by connecting a match massage for extended basic data and information stored in the simple basic data .[223]

Scrutinizing the provisions of Counter-terrorism database act with regard to the requirement of specificity and unambiguity, the Court considered that storing information on persons who merely support a supporting organization to terrorism was too broad and lacked subjective connection to terrorism.[224] Similarly, recording a person in a database for a mere "advocacy" of violence was overly vague, so as to give wider latitude to the security agencies and thus, do not comply with the principle of unambiguity.[225] Further, the possibility of including contact persons of the persons covered by the Act gives the executive free discretion as to what data may be stored as it fails to comply with the principle of predictability.[226]

As regards to the storage criteria on the other hand, provisions complied with the principle of specificity, as it does not require an absolute prohibition of vague terms as long as it does not

[221] Schwartz, Systematic Government Access to Private-Sector Data in Germany, 78.
[222] *Ibid.* 170.
[223] *Ibid.* 198.
[224] *Ibid.* 149.
[225] *Ibid.* 150.
[226] *Ibid.* 164.

jeopardize its predictability and judicial reviewability of executive acts.[227]An open-ended description of the data to be stored thus survived constitutional objection as it did not grant the blanket authorization to the security agencies but laid down the specific criteria for assessment supported by the examples which would further be defined by the executive according to its professional expertise.[228]

Due to the limited degree of transparency and legal protection with regard to the Counter-terrorism database, the Court stressed the heightened importance of practicable and effective supervisory oversight.[229] This would require supervisory authorities such as Data Privacy Commissioners to be equipped with effective powers. Keeping the records of accesses and modifications in the database and its availability to the Commissioner was to be ensured in order to enable meaningful evaluation and audit. [230] Further the Court required regular supervision with no longer the 2-years intervals as well as regular reports by the BKA to Parliament and the public on the contents and use of the counter-terrorism database.[231]

3.3.5 BKA Act Case

The final chapter in "a tale of gradual expansion" of powers of the BKA, the constitutional court was called upon to rule on the constitutionality of BKA Act, conferring BKA counter-terrorism competences and covert surveillance powers as well as the leading role in coordination and maintenance of the investigative data throughout Germany.[232] Covert Surveillance measures

[227] *Ibid.* 181.
[228] *Ibid.* 182.
[229] *Ibid.* 214.
[230] *Ibid.* 215.
[231] *Ibid.* 217.
[232] Miller, A Pantomime of Privacy: Terrorism and Investigative Powers in German Constitutional Law, 1552.

according to the new act included collection of personal data for the purposes of "protection against threats from international terrorism and the prevention of criminal offences".

The Court found the authorization for conducting secret surveillance measures to "protect against threats from international terrorism" to be in principle compatible with the Basic law but objected on the design of the investigative powers with respect to the principle of proportionality.[233] In its balancing exercise, the Court considered protection against interference with the right to privacy and especially the private refuges on the one hand, and the protection against threats to international terrorism to guarantee the safety of the population on the other as equally ranking constitutional interests.[234]

Reiterating its standards established by previous case-law, the court scrutinized individual provisions of the Act. First, it found "preliminary stages of a still vague and unforeseeable specific threat" to be disproportionately broad to provide basis for carrying out the special surveillance measures outside home.[235] Moreover, the Court objected on the lack of sufficient judicial oversight over monitoring and recording of non-public conversations and long-term observation including visual recording or the use of tracking devices were either wholly exempted or only require the judicial order only for its extension.[236]

The Court further required that, apart from emergencies, data collected as a result of surveillance in private homes be subject to prior verification by an independent body to review its legality and ensure that the information touching the core area of the private is not deployed by BKA.[237] In addition, the Court questioned the independence of the body responsible for

[233] 1 BvR 966/09 (2016).
[234] *Ibid.* 99.
[235] *Ibid.* 113.
[236] *Ibid.* 174.
[237] *Ibid.* 200.

screening the data collected through the information technology systems and required independent external control by persons unrelated to security matters.[238] The court found the extension of surveillance powers over on-going telecommunications and telecommunications traffic data for preventing criminal offences to be unspecific and disproportionately broad.[239]

According to the GCC, additional safeguards for the transparency, legal protection and judicial review were missing from the challenged law, specifically, conditions for regular mandatory review, documentation and reporting requirement.[240] The Court further found that keeping the data for the purposes of law-enforcement, crime prevention or future prosecutions could not possibly have a legal basis due to its broadness.[241] As regards to the purpose limitation, the Court considered that specific evidentiary basis for further investigation would be sufficient for the secondary use of the collected data.[242]

The Court found the provisions allowing a transfer of information to other domestic agencies unconstitutional for the purposes of general prevention of terrorist crimes, without regard to the concrete evidentiary basis for further investigations.[243] Furthermore, the Court found that effective oversight by the Federal Data Protection Commissioner was not sufficiently guaranteed by the data transfer provisions.[244]

[238] *Ibid.* 224.
[239] *Ibid.* 232.
[240] *Ibid.* 266.
[241] *Ibid.* 274.
[242] *Ibid.* 292.
[243] *Ibid.* 315.
[244] *Ibid.* 322.

3.4 Constitutional Court of Georgia

3.4.1 This affects you! they are still listening

Soviet legacy that Georgia had inherited had to be overcome by the new commitment to rule of law and human rights. Although these principles were enshrined in the Constitution in 1995, its effective implementation had been largely dependent on the development of democratic institutions and civil society movements, which has been a continuous, still on-going process. Against this backdrop, illegal surveillance had been a routine practice by the law-enforcement. Despite the fact that the threat of terrorist attacks is not as pressing in Georgia as in the U.S. and Germany, government officials try to justify its ever-increasing appetite for surveillance powers by Counter-terrorism objectives.[245]

Public outrage and intense campaigns against illegal government surveillances has prompted a review of surveillance legislation to address the problem of abuses. Until 2015, Georgian intelligence services were merged into ministry of interior creating a "powerful centralized system." One of the measures enacted in 2015 was the reform to decouple intelligence agencies from the police in order to de-concentrate an excessive power.[246] Consequently, separate State Security Service has been established, with the competences over counter-terrorism, counter-intelligence and anti-corruption measures. Government's claims about a positive shift from "repression-based police" to "preventative force", has however been overstated considering that

[245] As one of the leaders of parliamentary majority has stated after President vetoed the new surveillance law, "the President vetoed not the law but the safety of our citizens, fight against organized crime, and our ability to deal with the risks of terrorism." See Archil Talakvadze: The President Vetoed the Security of Our Citizens, *interpressnews.ge*, March 22, 2017, http://bit.ly/2eHIYaR

[246] Turashvili, Teona Iakobidze, Tamar, 2017. Regulating Secret Surveillance in Georgia (April-December, 2016), Institute for Development of Freedom of Information, 13 https://idfi.ge/en/regulating_secret_surveillance_in_georgia_media_coverage

the powers extended not only to intelligence-gathering but investigation and law-enforcement as well.[247]

Another change introduced by legislative amendments in 2015 envisaged the establishment of so-called two-key system, which was to enable personal data protection inspector to oversee proper execution of court orders.[248] The law however, was deficient in many respect, and consequently had been challenged before the constitutional Court of Georgia.[249]

3.4.2 Public defender of Georgia et al. v. Georgian Parliament

The Constitutional Court rendered a judgment upon the constitutionality of the amendments, which remains the major decision in the field of secret surveillance. The Court scrutinized the provisions regarding the powers of intelligence agencies to conduct real-time telecommunications surveillance and to that end, install technical equipment and programs directly to the communications facilities. These powers extended to wiretapping and collection of information from any telecommunications services, computer systems and networks, including internet and provided for direct access to communications data.[250] In addition, intelligence agency had been fully responsible for installment and administration of such technical infrastructure.[251]

The reasoning of the Court followed the same pattern of proportionality analysis as that of a German one. It emphasized, that the interference had to be envisioned by the law that is

[247] *Ibid.* 13
[248] Criminal Procedure Code of Georgia 332[3] 30.11.2014. №2870 https://matsne.gov.ge/ka/document/view/90034
[249] Turashvili, 3.
[250] Public defender of Georgia et al. against Georgian Parliament, II, 36.
[251] *Ibid.* 38

foreseeable and it could only be justified if the state deployed a least restrictive means for the achievement of the legitimate aim.[252] In addition, Court stressed that even though a judicial warrant was an essential prerequisite for permitting such measure, warrant alone would not suffice to curb government abuses if the law itself created the temptation for the excessive action going beyond the Constitutional Guarantees.[253] According to the Court, the law itself should not be provoking the violation.[254]

The Court pointed out that the Constitutional requirements were all the more demanding with regard to the secret surveillance measures due to the limited control and oversight possibilities. Regarding the direct access to communications facilities, the court quoted the ECtHR case law to highlight the especially high risk of abuse.[255] According to the Court, the law infringing upon the private sphere should comply with the principles of specificity, foreseeability and accessibility as additional requirements dictated by the rule of law. This is to ensure that the executive does not enjoy unfettered discretion to set the scope of its actions. Legislature is thus required to provide adequate guidelines for executive action in order to guarantee their predictability and reviewability in terms of their absolute necessity, appropriateness and legality as well as enable individuals to be aware of the measures they can be subjected to.[256]

The Court first recognized that, the access to real-time communications by the executive can be justified, as a last resort for effective investigation. However, empowering the investigative body to possess and administer technical means that enable such surveillance increased the risks

[252] *Ibid.* 40
[253] *Ibid.* 43
[254] Public defender of Georgia and others v. Georgian Parliament, II, 69.
[255] *Ibid.* II, 68.
[256] *Ibid.* II, 46.

of privacy violations and allowed the surveillance of unlimited number of persons.[257] This was true especially taking into consideration the fact that formation and functioning of such technical infrastructure was regulated by the Normative Act of the Head of the Agency itself, which was classified and that deployment of such infrastructure could not be audited by an independent body.[258] While acknowledging that in view of ever-growing technology, it is impossible to lay down all the technical requirements by the statute, this should not be understood as giving the executive an unlimited scope to decide when and how to deploy such means. [259]

In this respect, the Court stressed that that National Intelligence Agency was a professionally interested body in collecting as much information as possible to simplify crime prevention or investigation. In absence of the adequate safeguards, the temptation of unlawful and unjustified intrusion was consequently heightened.[260] Such an unfettered control by the investigative body itself, in view of the continuous advancement of surveillance techniques, created the serous weapon for phycological manipulation.[261] The Court thus concluded that existing provisions did not provide for sufficient external control to the use of surveillance techniques by intelligence agencies.[262]

Further examining the functioning of the two-key control system, the Court was not satisfied that the law sufficiently excluded the possibility of conducting secret surveillance outside constitutional boundaries, given that only those activities that came to the knowledge of the Personal Data Protection Inspector could be supervised.[263] Considering the fact that the law envisaged the oversight of Personal Data Protection Inspector only in relation to the specific

[257] *Ibid.* II, 53
[258] *Ibid.* 56.
[259] *Ibid.* 75.
[260] *Ibid.* 55.
[261] *Ibid.*
[262] *Ibid.* 55.
[263] *Ibid.* 60.

system and that intelligence agency was not limited to install alternative technical infrastructure, the oversight of the other techniques would have been impossible.[264] Other functions of the inspector were deemed ineffective as well, as declared by the Personal Data Protection Inspector, its oversight powers were slightly more than minimal.[265] Given that the two-key system is not applicable to internet traffic, the oversight of the Inspector is limited to the subsequent inspection of the legality of data processing.[266]

In view of all the above, the court considered that the interference was disproportionate, as the same aim could be achieved by a least restrictive means of elaborate system of safeguards which would minimize the risks of privacy intrusion.[267]

Another challenged provision enabled intelligence service to copy and store the communications proceedings including the time, location, duration, parties of the communication for two years.[268] The Court again objected on the involvement of the professionally interested body in such data processing and required that the data be handled by a sufficiently independent and effectively controllable organ.[269] One safeguard in place was the supervision of the data processing activities within the data banks by the Personal Data Protection Inspector, through electronic system.[270] This supervision could however be circumvented by creating alternative banks which would be inaccessible to Personal Data Protection Inspector and even outside the knowledge of communications service providers.[271] The Court added that Even the existing

[264] *Ibid.* 59.
[265] *Ibid.*
[266] *Ibid.* 76.
[267] *Ibid.* 81.
[268] *Ibid.* 85.
[269] *Ibid.* 97.
[270] *Ibid.* 99.
[271] *Ibid.*100.

electronic program to which the Inspector had access to, did not function well due to the technical problems.[272]

Concerned with the sheer quantity of the data that could be obtained and stored by the intelligence agencies, the Court concluded that a blanket authorization to gather unlimited amount of information about any person regardless to their connection to a criminal act or even the existence of an abstract danger for an "unreasonably lengthy period" was disproportionate.[273] The Constitutional court thus established the requirement that investigative body should not have a direct access to telephone and internet communications or the authority to to copy and store this information for long periods.[274]

3.4.3 New Law- New Complaint

Following the Judgment, the Parliament enacted a new law creating an Operative-Technical Agency which became responsible for communications surveillance which is still within the structure of State Security Agency.[275] "Strategic surveillance" has been added to its powers as a new measure, which involves surveillance of telecommunications outside Georgia and allows it to be carried out without prior judicial approval.[276] The law further modified the functions of

[272] *Ibid.* 103.
[273] *Ibid.* 109.
[274] *Ibid.* 97.
[275] Law of Georgia on LEPL Operative-Technical Agency, 03. 22. 2017. 475-IIS, http://info.parliament.ge/file/1/BillReviewContent/146594
[276] *Ibid.* Article 2 "a", https://matsne.gov.ge/a/document/view/3597534

Personal Data Protection Inspector[277] and established a new institute of "supervisor judge" who authorizes and oversees electronic surveillance measures.[278]

Despite the changes, and maybe even because of them, the new law did not meet the expectations of civil society representatives and was challenged before the Constitutional Court with the main objections over the lack of independence of the newly created body, its expanded powers and formal and ineffective safeguards. The case is yet to be decided by the Court and it remains to see what will see how far its constitutional review will go.

3.4.4 Comparison of Jurisprudence of German and Georgian Constitutional Courts

As discussed in the thesis, foundational similarities among the German and Georgian Constitutional protection of privacy is apparent. The case law of Georgian Constitutional Court seems to stay in line with this tendency. Common features of the Court decisions include the use of three-prong proportionality analysis together with the requirement to use least restrictive means for the infringement of the fundamental right and the principle of clarity and determinedness, which compel the legislature to put limits on executive action in a foreseeable manner. In this way, the Courts provide an important check to review the legislation that confers the executive too broad discretion to determine its scope of action and obstruct its reviewability.

Similarly, Courts in both jurisdictions have considered direct access to the unlimited amount of data by a professionally interested body especially problematic and recognized the need for an

[277] *Ibid.* Article 2, "I" "i.a" and "i.b"

[278] Law of Georgia on Counterintelligence Activities, Article 2, "n" "n.a" and "n.b" 11.11.2005, 2097, https://matsne.gov.ge/ka/document/view/27364#

independent external oversight. While deciding upon the constitutionality the Courts carefully examine additional safeguards for the access and subsequent use of data, its deletion requirement and so forth to assess the totality of the measure in terms of its proportionality.

4 Conclusion

Looking into the development of privacy regimes in three jurisdictions, it becomes apparent that without meaningful constitutional review, the natural tendencies of the executive to expand its surveillance powers, especially taking advantage of the crisis situations, often finds support by the legislature. The role of the Supreme/Constitutional jurisprudence to place governmental power within the Constitutional boundaries is thus significant.

Despite American libertarian principles focusing on constraining the state power, in the context electronic surveillance the Supreme Court has failed to address the contemporary challenges. By contrast, inheritance of the totalitarian past has been effectively overcome by the renewed commitment to the centrality of human personality and the rule of law trough the elaborate jurisprudence Constitutional Courts of Germany and Georgia.

Critics of the German Constitutional Court have claimed that its judicial activism excessively intruded upon the competences of the political branches, dictating the conditions for legislative action.[279] Conversely, in view of the increasingly blended police and intelligence functions, the Court has also been criticized to be more focused on the insignificant technicalities such as deletion declines and the like, than the meaningful judicial review of the infringing measure. [280] It remains to be seen what the take on the Georgian Constitutional Court in its pending case will be, the focus on the oversight measures and the clearly specified conditions for the access and the use of data is however the best attempt to achieve a balanced trade-off between the privacy and security.

[279] Paul M. Schwartz, Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the States, and New Technology, William & Mary Law Review. 2011, Vol. 53 Issue 2, p351-387. 384
[280] Russell A. Miller, A Pantomime of Privacy: Terrorism and Investigative Powers in German Constitutional Law, Boston College Law Review. 2017, Vol. 58 Issue 5, p1545-1628.

Bibliography:

Case Law:

Berger v. New York, 388 U.S. 41 (1967)

BVerfGE 65, 1. (1983)

1 BvR 370/07 (2008)

1 BvR 256/08 (2010)

1 BvR 1215/07 (2013)

1 BvR 966/09 (2016)

Georgian Citizens – Alexandre Macharashvili and Davit Sartania v. Georgian Parliament and Ministry of Justice, Constitutional Court of Georgia, 1/2/458. (2009)

Georgian Young Lawyers Association and Ekaterine Lomtatidze against Parliament of Georgia, Constitutional Court of Georgia N1/3/407. (2007)

Goldman v. United States, 316 U.S. 129 (1942).

Katz v. United States, 389 U.S. 347 (1967)

Kyllo v. United States, 533 U.S. 27 (2001).

Olmstead v. United States, 277 U.S. 438 (1928)

Payton v. New York, 445 U.S. 573 (1980).

Public defender of Georgia et. al against Georgian Parliament, Constitutional Court of Georgia 1/1/625, 640 (2016).

Smith v. Maryland, 442 U.S. 735 (1979)

United States v. Jones, 565 U.S. 400 (2012).

United States v Karo, 468 U.S. 705 (1984).

United States v. Knotts, 460 U.S. 276 (1983).

United States v. Miller, 307 U.S. 174 (1939)

United States v. United States Dist. Ct., 407 U.S. 297 (1972)

Legislation

Foreign Intelligence Surveillance Act (FISA) of 1978; Public Law 95-511; 92 STAT. 1783

Law on Counterintelligence Activities, 11.11.2005, 2097

Law of Georgia on Electronic Communications, 06.06.2005, 1514

Law of Georgia on LEPL Operative-Technical Agency,03.22.2017. 475-IIS

Omnibus Crime Control and Safe Streets Act of 1968; Public Law 90–351; 82 Stat. 197

Uniting and Strengthening America by Fulfilling Rights and ensuring Effective Discipline over monitoring Act of 2015; Public Law 114–23; 129 STAT. 268

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001; Public Law 107–56; 115 STAT. 272

Books

Burduli Irakli, Gotsiridze Eva, Erkvania Tinatin, Zoidze Besarion, Izoria Levan, Kobakhidze Irakli, Loria Archil, Matcharadze Zurab, Turava Merab, Phirtskhalashvili Ana, Futkaradze Iakob, Kantaria Beqa, Tsereteli Davit, Jorbenadze Sandro. *Constitutional Commentaries – Chapter two, Georgian Citizenship and Basic Human Rights and Freedoms*. Tbilisi: Petiti Pres, 2013.

Davis, Fergal, McGarrity, Nicola and Williams Abingdon. Eds. *Surveillance, Counter-terrorism and Comparative Constitutionalism*, George. Oxon: Routledge, 2014.

Zeugmann, Cora. *The Trade-Off between Civil Liberties and Security in the United States and Germany after 9/11/01*, Hamburg: Diplomica Verlag. 41. 2008.

Davis, F, McGarrity, N, and Williams, G. *Surveillance, Counter-Terrorism and Comparative Constitutionalism*, Abingdon, Oxon: Routledge 2014.

Gray, David C. *The Fourth Amendment in an age of surveillance*. Cambridge: Cambridge University Press, 2017.

Kommers, Donald P. *The constitutional jurisprudence of the Federal Republic of Germany*. Durham: Duke University Press, 1997.

Rau, Markus. "Country Report on Germany," in Terrorism as a challenge for national and international law: security versus liberty? Eds. Walter, Christian, Voneky, Silja, Roben, Volker, 2004.

Sarat, A. *World Without Privacy: What Law Can and Should Do?*. New York, NY: Cambridge University Press, 2015.

Solove, Daniel J., Rotenberg, Marc and Schwartz, Paul M. *Privacy, information, and technology*. New York: Aspen Publishers, 2006.

Solove, Daniel. *Understanding Privacy*. Cambridge, Mass.: Harvard University Press, 2008.

Schwartz, Paul M. "Systematic Government Access to Private-Sector Data in Germany," in Bulk Collection: Systematic Government Access to Private-Sector Data, Oxford University Press. 2017.

Westin, Alan F. *Privacy and freedom.* New York: Athenium, 1967.

Journal Articles

Bloom, Robert. Dunn, William J. The Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment, *William & Mary Bill of Rights Journal*. 15 (2006), 147-202.

Barnum, David G. "Judicial Oversight of Interception of Communications in the United Kingdom: An Historical and Comparative Analysis null." *Georgia Journal of International and Comparative Law*, no. 2 (2015) 237-304.

Barnum, David G. "Warrantless Electronic Surveillance in National Security Cases: Lessons from America." *European Human Rights Law Review* 5 (2006) 514-540.

Bignami, Francesca. "European versus American Liberty, a Comparative Privacy Analysis of Antiterrorism Data Mining." *Boston College Law Review* 48, no 3 (2007) 609-698.

Eberle J. Edward. "Human Dignity, Privacy, and Personality in German and American Constitutional Law." *Utah Law Review*. 1997, (1997) 963-1056.

Gerrit, Hornung and Schnabel, Christoph. Data protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law and Security Review: The International Journal of Technology and Practice*, 25, no 1 (2009), 84-88.

Hornung, Gerrit; Schnabel, Christoph, "Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention", *Computer Law and Security Review: The International Journal of Technology and Practice*, 25, no 2 (2009) 115-122

Jacoby, Nicole. "Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and United States", *Georgia Journal of International & Comparative Law.* 35, no 3 (2007) 431-493

Whitman, James Q. "The Two Western Cultures of Privacy: Dignity versus Liberty." *The Yale Law Journal* 113, no 6 (2004) 1151-1221.

Schwartz, Paul M. "Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the States, and New Technology." *William & Mary Law Review*. 53, no 2 (2011) 351-387.

Schwartz, Paul. M. German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance, *Hastings Law Journal*, 54, no 4 (2002) 751-804.

Solove, Daniel J. Data Mining and the Security-Liberty Debate, *University of Chicago Law Review*, 75 no 1 (2008) 343-362.

Schwartz, P, "Evaluating Telecommunications Surveillance in Germany: The Lessons of the Max Planck Institute's Study," *George Washington Law Review* 72, no 6 (2004) 1244-1263.

Solove, Daniel J. "'I've Got Nothing to Hide" and Other Misunderstandings of Privacy', *San Diego Law Review*, 44, no 4 (2007) 745-772

Miller, Russell A. Balancing Security and Liberty in Germany. *Journal of National Security Law & Policy.* 4, no 2 (2010) 369-396.

Miller, Russell A. A Pantomime of Privacy: Terrorism and Investigative Powers in German Constitutional Law. *Boston College Law Review*. 58, no 5 (2017) 1545-1628.

Zoller, Verena, Liberty dies by inches: German counter terrorism measures and human rights. *German Law Journal*. 5 no 5 (2004) 469-494.

Online Sources

Giorgi Beraia, Tamar Iakobidze, Teona Turashvili, "Regulation of Secret surveillance in Georgia", Institute for development of Freedom of Information, January-August 2017, https://idfi.ge/public/upload/IDFI_Photos_2017/rule_of_law/surveillance_report_geo.pdf

Institute for Development of Freedom of Information, Regulating Secret Surveillance in Georgia: 2013-2015, May 2015. https://idfi.ge/public/upload/surveillance/Surveillance-final-28-03-2016.pdf

Hammarberg, Thomas. Georgia in transition. Report on the human rights dimension: background, steps taken and remaining challenges Assessment and recommendations, 2013, http://eeas.europa.eu/archives/delegations/georgia/documents/human_rights_2012/20130920_report_en.pdf;

The New York Times, House Extends Surveillance Law, Rejecting New Privacy Safeguards, last modified in Jan. 11, 2018 https://www.nytimes.com/2018/01/11/us/politics/fisa-surveillance-congress-trump.html

Putter, Norbet. The Federal Republic's security services from the Cold War of the "new security architecture", Statewatch Journal, 19 no 4. http://www.statewatch.org/analyses/no-102-germany-security-services.pdf