Privacy and Data Protection by Rules Rather Than Principles

*Axel Tschentscher**

Abstract: There is hardly any field of the law that has more diversity on both sides of the Atlantic than privacy and data protection. Common opinion often reduces that diversity to a matter of "strong" protection in Europe versus "weak" protection in the United States of America. Discussions about Safe Harbor and Privacy Shield regulation reinforce this perception. This paper, however, argues that the privacy divide is hardly a matter of strong or weak protection, but has deeper roots in different approaches to constitutional rights. While Europe, following the lead of the German Federal Constitutional Court, conceptualizes legal precepts about privacy and data protection as principles with a broad protective scope that result in balancing procedures, the protection in the U.S. is rule based. This results in a more rigid system with stronger emphasis on the legislatures of the states rather than flexible adjudication by the courts.

I. Civil Rights: Rules or Principles?

Contemporary European privacy protection has its origin in the right to autonomy about personal information (*Informationelles Selbstbestimmungsrecht*) acknowledged by the German Federal Constitutional Court in the census decision of 1983.[1] Following the constitutional rights theory of *Robert Alexy,* that right is conceptualized as a legal principle requiring the optimization of its normative content (*Optimierungsgebot*).[2] Legal principles in this sense are necessarily connected to balancing during application: where principles collide, balancing is the mode of application, where rules collide, the result is achieved by applying the rule that takes precedence over

* Professor for Constitutional Law, Legal Philosophy and Constitutional History at the University of Bern (Switzerland); the author extends his thanks to the members of the Privacy Research Group at New York University (www.law.nyu.edu/centers/ili/people), particularly the organizers of the 2015/16 sessions: *Helen Nissenbaum, Katherine Strandburg* and *Ira Rubinstein*. An abbreviated version of this paper has been published in German: Martin Borowski/Stanley L. Paulson/Jan.-R. Sieckmann (eds), Legal Philosophy and Constitutional Rights Theory [Rechtsphilosophie und Grundrechtstheorie], Tübingen: Mohr Siebeck 2017, at 563 ff.

[1] BVerfGE 65, 1 (43 ff.) – Census (*Volkszählung*) = www.servat.unibe.ch/dfr/bv065001.html.

[2] *Robert Alexy,* Theory of Constitutional Rights [Theorie der Grundrechte], 3rd ed. 1996 (3rd reprint 2011), at 75.

source: https://doi.org/10.7892/boris.120028 | downloaded: 24.4.2024

countervailing rules.[3] Balancing of legal principles follows a three-pronged proportionality test within constitutional law.[4] The third part of this test has been named the "balancing law" in legal scholarship: "The higher the degree of non-realization of one principle might be, the higher the importance and realization of the countervailing principle must be."[5] In principle based adjudication both sides of the norm collision retain some effect whereas rule base adjudication simply applies the "stronger" norm.

With few exceptions[6] constitutional rights are understood as legal principles in Germany, leading to balancing in nearly all cases. The Federal Constitutional Court works as the final arbiter of this balancing procedure, thereby taking precedence, in application of constitutional rights, over all other state institutions including the Federal Parliament. This implicit tendency towards a legal system run by its constitutional court has raised strong criticism against the theory of legal principles in constitutional rights theory in Europe.[7] In the United States, scholars are even more skeptical regarding the balancing procedure triggered by the theory of legal principles. They abhor the resulting self-empowerment of the Constitutional Court in Germany and fear a "viral" extension of this concept to other constitutional courts in the world at large.[8]

In light of that criticism, this paper asks about the alternatives the skeptics can offer for the adjudicative procedures of constitutional rights. What other tests are

---

[3] *Martin Borowski,* Constitutional Rights as Principles [Grundrechte als Prinzipien], 2nd ed. 2007, at 115.

[4] *Robert Alexy,* Human Dignity and Proportionality [Menschenwürde und Verhältnismäßigkeit], in: AöR 140 (2015), at 497-513 (501); differing only in detail: *Borowski,* Constitutional Rights as Principles (n. 3), at 120 f.: balancing only in the third part of the three-pronged test.

[5] *Alexy,* Theory (n. 1), at 146; *idem,* Human Dignity (n. 4), at 501.

[6] No balancing is allowed for the right to human dignity, the prohibition of capital punishment, the prohibition of torture and for the prohibition of censorship. The guarantee of the essentials of constitutional rights *(Wesensgehaltsgarantie)* results in a core protection for every constitutional right that also is rule based. Finally, the duty to optimize the normative content of legal principles is itself a rule, not a principle; see *Borowski,* Constitutional Rights as Principles (n. 3), at 92.

[7] E.g., *Ralf Poscher*, Constitutional Rights as Defensive Rights. Reflexive Regulation of Freedom Organized by Law [Grundrechte als Abwehrrechte. Reflexive Regelung rechtlich geordneter Freiheit], 2003, particularly at 75-76, 81-82; *Matthias Jestaedt,* Balancing Theory – Its Strengths and Weaknesses [Die Abwägungslehre – ihre Stärken und ihre Schwächen], in: Festschrift for Isensee, 2007, at 253 ff. (269 f.); *Wolfram Cremer,* Practical Concordance as a Rule to Resolve Conflict – How Legislative Fiat Gets Leveled [Praktische Konkordanz als grundrechtliche Kollisionsauflösungsregel – Einebnung gesetzgeberischer Entscheidungsspielräume], in: Festschrift for Jarass, 2015, at 175 ff. (180 f.); all with further references. As a general criticism against strengthening the courts within the balance of powers, but not yet focused on the matter of constitutional rights as principles: *Ernst-Wolfgang Böckenförde,* Constitutional Rights as Fundamental Norms. Regarding the Current Situation of Constitutional Rights Scholarship [Grundrechte als Grundsatznormen. Zur gegenwärtigen Lage der Grundrechtsdogmatik], in: Der Staat 29 (1990), at 1 ff. (25).

[8] *Alec Stone Sweet/Jud Mathews,* Proportionality Balancing and Global Constitutionalism, in: Columbia Journal of Transnational Law 47 (2008), at 72 ff. (156).

applied when abstaining from balancing? Do these tests actually lead to different results or are they just different approaches with similar or equal outcomes?

For comparative constitutional analysis regarding the rules vs. principles divide, the privacy and data protection in the United States of America is a most promising subject. The U.S. Supreme Court has an adjudicative power and institutional standing that matches and predates the Constitutional Court in Germany. Also, on both sides of the Atlantic, privacy protection has been developed and extended for many years by the case law of the courts rather than by constitutional amendments. This case law is still in the process of dynamic development thanks to the ever growing challenges of the internet age. The centuries of court run development of privacy law in the United States are comparable to what took place in Europe during the last three decades since the establishment of the right to informational autonomy. However, in stark contrast to Europe, the U.S. courts have adopted a rule based approach that tries to abstain from balancing wherever possible. To contrast privacy and data protection in the U.S. with the balancing approach in Europe therefore will help to understand the systemic differences both in procedure and in outcome.

II. Privacy and Data Protection in the United States: An Overview

1. Federal Constitutional Law

The U.S. Constitution does not contain a general rule about privacy and data protection. Rather, it protects privacy as an aspect of different provisions among the amendments.[9] The Fourth Amendment regarding unreasonable searches and sei-

[9] Among the amendments adopted as the US Bill of Rights in 1791 are the following parts entailing privacy protection (italics): "(1) Congress shall make no law respecting an establishment of *religion*, or prohibiting the free exercise thereof; or *abridging the freedom of speech,* or of the *press*; or the right of the people peaceably to *assemble*, and to petition the Government for a redress of grievances. (2) [...] (3) No Soldier shall, in time of peace be *quartered in any house, without the consent of the Owner,* nor in time of war, but in a manner to be prescribed by law. (4) The right of the people to be secure in their persons, houses, papers, and effects, *against unreasonable searches and seizures,* shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation and particularly describing the place to be searched, and the persons or things to be seized. (5) No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; *nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law;* nor shall private property be taken for public use, without just compensation. [...] (14) Sec. 1: All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United

zures is the most frequently applied provision in privacy cases. It has been broadly extended outside of the privacy context before, for instance to drunk driving tests as a form of search and to arrests as a form of seizure regarding the person.

The First Amendment regarding free speech, free press and free exercise of religion has an indirect implication for privacy protection. The right entails the privacy of one's belief as well as the right to anonymous speech. It also prohibits any kind of state action that results in chilling effects on these rights. Finally, the First Amendment guarantees the right to association that also grants protection against government acquisition of associational information.[10] In particular, that right might have the potential to limit the Government's power to indiscriminately collect communication metadata now to eventually use it for criminal prosecution in the future.[11]

The Third Amendment about the involuntary quartering of soldiers includes an even more tenuous protection of privacy. It is the basis for the privacy only within spaces used as living quarters.

Finally, the Fifth Amendment has some bearing on privacy because it protects against the involuntary disclosure of self-incriminating information. This amendment together with the due process clause of the Fourteenth Amendment requires fair procedures regarding all limitations of personal freedom.

2. State Constitutional Law

Only some state constitutions explicitly provide for the right to privacy within their basic rights catalogs. If mentioned at all, privacy protection is positioned among the new features at the end of the rights section. The Constitution of California, for instance, now includes privacy among the inalienable rights. Like an afterthought, however, it is appended at the end of the respective list.[12] The original version of the 1880 Constitution of California did not yet include that right.

The Constitution of Louisiana was amended in a similar way.[13]

States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; *nor shall any State deprive any person of life, liberty, or property, without due process of law;* nor deny to any person within its jurisdiction the equal protection of the laws. Sec. 2-5: [...]."

[10] *NAACP v. Alabama,* 357 U.S. 449, 462 (1958); *Shelton v. Tucker,* 364 U.S. 479 (1960); *Baird v. State Bar of Arizona*, 401 U.S. 1 (1971); *see Daniel J. Solove,* The First Amendment as Criminal Procedure, 82 N.Y.U. L. REV. 112 (2007) at 147 ff.

[11] *Cf. Katherine J. Strandburg,* Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance, 49 B.C. L. REV. 1 (2008); *idem,* Membership Lists, Metadata and Freedom of Association's Specificity Requirement," 10 *I/S: J.L. & Pol'y Info. Soc'y* 327 (2014).

[12] Art. 1 Sec. 1 CA-Const.: "All people are by nature free and independent and *have inalienable rights.* Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, *and privacy.*"

[13] Art. 1 Sec. 5 LA-Const.: "Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, *or invasions of privacy.* [...]."

In Florida's Constitution the right to privacy was also added at the end of the rights section. In this case, it was combined with a clarifying sentence regarding the right to obtain access to public records.[14]

Montana and South Carolina have opted to include privacy protection in the context of the rights against unreasonable searches and seizures.[15]

Alaska, Arizona, Hawaii, Illinois, and Washington have each used one of these amendment techniques. The other states followed the example of the Federal Constitution in protecting privacy implicitly through other constitutional rights.[16]

3. Federal Statutes

There is no federal statute containing a general provision about privacy or data protection as the data protection statutes in Europe usually do.

The most general of the federal statutes, the *Privacy Act of 1974,* focuses on rules about transparency and the right to correct errors in data. The act only applies to the activities of federal agencies. There are few prohibitions adopted in this act, for instance the prohibition to request the social security number as a prerequisite to granting rights, benefits, or privileges.[17] The sale of names and addresses of citizens is prohibited, but subject to the exception of specific authorization.[18] This prohibition of selling mailing lists is in itself only necessary because U.S. public administrative law does not contain a general requirement that agencies restrict their activities to what they are tasked with explicitly by the law. Accordingly, the requirement of strictly restricting the use of data to legal purposes, as was acknowledged in some cases, has only little effect on privacy and data protection at large.[19] Each agency has the power to decide about legal purposes within their general tasks, thereby claiming legitimate use of data for most of its activities (rou-

---

[14] Art. 1 Sec. 23 FL-Const.: "Every natural person has the *right to be let alone and free from governmental intrusion into the person's private life* except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law."

[15] Art. II Sec. 10 MT-Const.: "The *right of individual privacy* is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest." Art. 1 Sec. 10 SC-Const.: "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and *unreasonable invasions of privacy* shall not be violated, [...]."

[16] *Cf. Dominika Blonski,* Biometric Data as a Subject of Informational Autonomy [Biometrische Daten als Gegenstand des informationellen Selbstbestimmungsrechts], 2015, at 154 ff.

[17] Federal Privacy Act of 1974, Sec. 7(a)(1): "It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number."

[18] Federal Privacy Act of 1974, 5 U.S.C. § 552a(n): "An individual's name and address may not be sold or rented by an agency unless such action is specifically authorized by law. [...]".

[19] Vgl. *Christopher W. Wasson,* Privacy Law – The Routine Use Exception to the Privacy Act: A Clarification on Compatibility, in: Villanova Law Review 35 (1990), at 822 ff.

tine use exception).[20] Furthermore, the protective power of the Privacy Act as well as other statutes – and even of constitutional privacy and data protection[21] – is restricted to U.S. citizens and resident aliens.[22] The Privacy Act, therefore, does neither grant strong protection nor does it direct the protective force in the way of a human right acknowledged for all of mankind.

The more specialized statutes within federal law do provide for more effective privacy and data protection. Their protection is targeted not only against public agencies, but also against corporations and other private actors.

Since 2005, for instance, the *Federal Credit Reporting Act of 1970* established a very effective individual right to free file disclosure that entitles consumers to free and centralized information about the underlying facts of their credit history as registered with the three big U.S. credit rating agencies.[23]

The *Health Insurance Portability and Accountability Act of 1996* protects the privacy and data autonomy of non-consenting patients by strictly restricting the use of protected health information to important issues of public health, victimization, and law enforcement.[24]

Similarly, the *Cable Communications Policy Act of 1984* provides for a restriction of data use by cable companies to the services offered as long as there is no prior written or electronic consent of the subscriber to more extensive use of their personally identifiable information.[25]

4. State Statutes

Among the statutes of the states, California has probably the most extensive and advanced privacy regulation. It frequently sets the standard for regulation in other states. Regarding data protection, many states followed California in adopting a duty to immediate information of customers in case of a data breach (breach notification). Even the European Union now adopted a similar rule as part of the *General Data Protection Regulation (GDPR)* that will be in force starting 25 May 2018.[26]

---

[20] *Blonski,* Biometric Data (n. 16), at 171 f.

[21] *See United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990), at 259 ff. (267): "There is likewise no indication that the Fourth Amendment was understood by contemporaries of the Framers to apply to activities of the United States directed against aliens in foreign territory or in international waters."

[22] 5 U.S.C. (n. 18), § 552a(a)(2): "the term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence; [...]".

[23] Federal Credit Reporting Act of 1970, 15 U.S.C. § 1681j(a).

[24] Health Insurance Portability and Accountability Act of 1996, 45 C.F.R. § 164.512.

[25] Cable Communications Policy Act of 1984, 47 U.S.C. § 551(c).

[26] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Art. 33 (1): "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority [...].", and Art. 34 (1): "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communi-

The breach notification rule is often combined with the promise of immunity from criminal prosecution as long as safety standards and other rules are observed (safe harbor).

5. Common Law

The earliest source for legal protection of privacy is the common law. In its 1890 article titled "The Right to Privacy", *Warren* and *Brandeis* have established the right to be let alone as a legal claim based in common law.[27] Originally, the authors were only concerned with legal protection against undue privacy interference by press journalists and photographers. *Brandeis,* in his office as Justice of the U.S. Supreme Court, later established privacy protection as a constitutional right against undue state interference. His dissenting opinion in *Olmstead* – that would become a landmark for privacy evolution – claims a violation of the Fourth Amendment in the case of warrantless phone tapping by the Federal Police.[28] The common law roots remained alive and relevant even today. During the revival of privacy litigation in the 1960s, the majority in *Griswold* appealed to the long tradition of that right being "older than the Bill of Rights".[29] As a common law right, privacy enjoys a generality that is independent of its ties to specific amendments. The U.S. Supreme Court used that generality in its pornography jurisdiction when differentiating between regulation at large and regulation extended to the private sphere of the home.[30]

III. The Rule-Exception-Character of Privacy Tests

Among the tests for the constitutional right to privacy the *reasonable expectation* criterion works as an entry point. It has been developed in *Katz* where warrantless

---

cate the personal data breach to the data subject without undue delay." The *GDPR* replaces the old *Data Protection Directive* of 1995 that did not yet contain these breach notification rules.

[27] *Samuel D. Warren/Louis D. Brandeis,* The Right to Privacy, in: Harvard Law Review 4 (1890), at 193 ff.

[28] *Olmstead v. United States,* 277 U.S. 438 (1928), at 471 ff. (478 f.): "To protect, that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence | in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth."

[29] *Griswold v. Connecticut,* 381 U.S. 479 (1965), at 479 ff. (486): "We deal with a right of privacy older than the Bill of Rights ...". The extension of that right to persons independent of the bond of marriage was acknowledged in *Eisenstadt v. Baird,* 405 U.S. 438 (1972), at 438 ff. (439).

[30] *Stanley v. Georgia,* 394 U.S. 557 (1969), at 557 ff. (565): "Whatever may be the justifications for other statutes regulating obscenity, we do not think they reach into the privacy of one's own home."

phone tapping by the police was classified as a violation of the *search and seizure* rule of the Fourth Amendment.[31] According to the concurring opinion of *Justice Harlan,* the formula *"reasonable expectation of privacy"* comprises two preconditions for constitutional protection.[32] On the side of the person protected, that person must have exhibited an actual expectation of privacy. And from the viewpoint of society, that expectation must reasonably deserve protection. Whoever is talking within a closed phone booth has this kind of reasonable expectation of privacy, whereas such expectation would not be reasonable if the communication took place without any protection among the general public. A large number of Supreme Court decisions have elaborated on this distinction.[33]

The *reasonable expectation* criterion as well as the Fourth Amendment privacy right both work as legal rules, not as principles. This is witnessed by the obvious lack of balancing in the application of these precepts. The practical importance and, therefore, weight of the public interest in wiretapping does not come into play. As long as the conditions to apply the criterion or right are fulfilled, the legal effect arises in an all-or-nothing fashion rather than as a matter of degrees. Whoever criticizes the decision about a case at hand will equally resort to rule oriented arguments. The dissenting opinion of *Justice Black* in *Katz,* for instance, focused on the formula "reasonable expectations" being too broad because immaterial communication was not tangible in the same way as physical things are.[34] This rule model of constitutional right leads to an all-or-nothing in the application of the law. It is averse to balancing. As long as the conditions for constitutional protection are met, the legal right has to be granted no matter how strong the infringement affects the person or how much weight the countervailing public interest has.

Admittedly, the application of the *reasonable expectation* criterion is subject to legal exceptions. This, however, even strengthens the argument about the rule character in U.S. constitutional rights application because the exception itself also partakes in this character. Among the rules constituting privacy exceptions are the exclusion of foreigners mentioned before[35] and, most importantly, the *third party doctrine*. According to that exception privacy protection does not arise for information freely provided by the person to any third person. If, for instance, Government authorities do not seize the files of the person directly, but obtain access to files held by the bank of that person, i.e., receive indirect access to the same infor-

---

[31] *Katz v. United States,* 389 U.S. 347 (1967).

[32] *Katz v. United States,* 389 U.S. 347 (1967), at 361.

[33] *United States v. White,* 401 U.S. 745 (1971); *United States v. Karo,* 468 U.S. 705 (1984); *California v. Ciraolo,* 476 U.S. 207 (1986); *Kyllo v. United States,* 533 U.S. 27 (2001); *United States v. Jones,* 132 S.Ct. 945 (2012); *Florida v. Jardines,* 133 S.Ct. 1409 (2013); *Riley v. California,* 134 S.Ct. 2473 (2014).

[34] *See* the dissenting opinion of *Justice Black* in Katz *v. United States,* 389 U.S. 347 (1967), at 364 pp (365).

[35] *See supra* n. 22.

mation, then this access is exempt from privacy protection.[36] In the case of phone records, this exemption has led to the Government's unrestricted access to metadata.[37] The same rationale currently applies to internet access data collected by internet service providers (customer's ip numbers, logs with ip numbers etc.).

The legal exception constituted by the *third party doctrine* has itself rule character. Applying this doctrine does not involve the relative weight of the right to privacy on the one hand and the Government's interest in obtaining information on the other. No matter how important the privacy interest and no matter how unimportant the information gathering interest, the exception will apply once the data is freely provided to a third person. As a result, the Government is not constitutionally restricted in using personal information that is provided due to contractual obligations or for other legal reasons.

This holds true even in extreme cases. If a university has access to the password protected laptop of a researcher who also uses that computer for private purposes, that person, according to *third party doctrine,* cannot claim a constitutional right to privacy against the police.[38] Federal law does provide for some protection even in cases of third party access.[39] But that protection does not have the same priority over statutes that a constitutional right can guarantee. It is in itself subject to more specialized regulation in federal law acknowledging unrestricted Government access. In effect, there is no control by the U.S. Supreme Court once the protection is outside of the scope of constitutional rights.

Because of the rule character of *third party doctrine*, the Fourth Amendment looses a large part of its privacy protection without ever resorting to balancing and, therefore, without distinguishing cases of highly sensitive data (e.g., the private use of a university laptop for e-mails, social media, and diary entries) from more general personal information provided to third parties (e.g., driving data for car insurances). And again: the critics are staying within the rule oriented approach to privacy law when merely objecting to the scope of the exception. In the critical opinion by *Justice Sotomayor* in *Jones*,[40] for instance, the application of the rule to the in-

---

[36] *United States v. Miller,* 425 U.S. 435 (1976), at 435 ff. (435): "The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."

[37] *Smith v. Maryland,* 442 U.S. 735 (1979), at 735 ff. (744): "This analysis dictates that petitioner can claim no legitimate expectation of privacy here. When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed."

[38] *United States v. Yudong Zhu,* 41 F.Supp.3d 341 (S.D.N.Y. 2014).

[39] Federal Wiretap Act of 1968, 18 U.S.C. §§ 2510 ff.

[40] *United States v. Jones,* 132 S.Ct. 945 (2012) – concurring opinion of *Justice Sotomayor:* "More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. [...] This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."

ternet is questioned, but not the general character of the exception as such. Even if *third party doctrine* would be restricted to the bricks and mortar world of the pre-internet times, its character as an all-or-nothing precept could not be changed. There still would be no balancing in applying *third party doctrine*.

IV. The Difference Between Rule Based and Principles Based Constitutional Protection

The constitutional privacy and data protection in the United States of America can be compared to that of Germany and Europe only indirectly. The interpretation and application of constitutional rights follows a different theory on both sides of the Atlantic. The rule based approach leads to an *inside theory* of constitutional rights protection. According to that theory, the constitutional right itself, the claim right, already comes complete with all its built-in conditions and restrictions. The scope of constitutional protection within a subject matter, e.g., in the field of privacy, ends at the border of a "preformed" sphere of legitimate claims.[41] Constitutional interpretation thereby arrives at a complete set of rules about application and exemption that define the constitutional right. This is the *effective scope* of constitutionally guaranteed protection Government must respect *("effektiver Garantiebereich")*. Even though it would be possible to include balancing within this approach, it usually has no place here, because the *inside theory* is streamlined towards rules in order to avoid the legal uncertainties that come with balancing.

German and European constitutional law follows – with few exceptions[42] – the *outside theory* of constitutional rights protection. This theory starts with a broad *prima facie* claim right.[43] This *prima facie* claim to constitutional protection arises whenever a Government activity infringes on the personal and material protective scope of the constitutional right *("Schutzbereich")*. Since the protective scope of individual rights protection is construed broadly, the public interest frequently requires limits to what actually can be upheld as effective protection under the claim. Therefore, in a second step of the outside theory of constitutional rights application, the *prima facie* claim right needs to be reduced to a definitive claim right. This is done by asking about the relative importance of Government regulation as opposed to the weight of the claim right, i.e., its proportionality *("Verhältnismässigkeit")*. In the end, both the outside and inside theory lead to a definitive answer to the question about

---

[41] For a general analysis notwithstanding U.S. law: *Gertrude Lübbe-Wolff*, Constitutional Rights as Rights to Defend Against Government Infringements. Structure and Scope of the Scholarship About Infringements in the Case of Public Benefits [Grundrechte als Eingriffsabwehrrechte. Struktur und Reichweite der Eingriffsdogmatik im Bereich staatlicher Leistungen], 1988, at 17.

[42] *See supra* n. 6.

[43] *Borowski,* Constitutional Rights as Principles (n. 3), at 34 ff. m.w.N.

the effective scope of constitutionally guaranteed protection. But the procedure to arrive at this answer is different.

The two step procedure involving a *prima facie* claim and a definitive claim could, in theory, be redefined as a complicated network of rules and exceptions capturing both the rise of the claim and its reduction to the scope of definitive protection. In the reality of constitutional law, however, this is not done. Rather, the two step procedure falls into symbiotic relationship with principles theory and resorts to balancing. The Government's power to legitimately reduce the *prima facie* claim right by legislation or by administrative acts requires proportionality, i.e., the relative importance of Government activity as opposed to the weight of the constitutional right. Principles theory bases that requirement on the character of constitutional rights as legal principles. Rather than granting protection in an all-or-nothing fashion, principles further the protective goals of constitutional rights as far as possible *relative* to the public interest. This is what the "balancing law" in legal scholarship expresses.[44]

The balancing procedure is pervasive in the realm of privacy and data protection. In its most recent case about the Federal Criminal Police Statute (BKAG), the German Federal Supreme Court has consolidated its line of adjudication in that regard.[45] By applying the balancing procedure within the proportionality requirement the court has forced the legislature to reduce its approach to surveillance and prosecution relative to the weight of the Government's infringement of privacy.[46] This balancing resulted in a number of specific requirements about transparency, information, jurisdiction, effectiveness of sanctions, and the right to have personal data erased.[47] There is a core of intense privacy protection that is, due to its connection to human dignity,[48] more than a *prima facie* claim right and cannot be further reduced by balancing.[49] But even this scope of core privacy depends on "in what kind and intensity it affects, by itself, the sphere of others or of the community".[50] Therefore, even the limit to the balancing procedure is determined by a balancing procedure.

---

[44] *See supra* definition in text at n. 5.

[45] BVerfGE 141, 220 – BKAG with references to prior case law = www.servat.unibe.ch/dfr/bv141220.html.

[46] BVerfGE 141, 220 (266 ff.) – BKAG.

[47] BVerfGE 141, 220 (282 ff.) – BKAG

[48] BVerfGE 109, 279 (313 ff.) – Intruding Surveillance [Großer Lauschangriff] with further references = www.servat.unibe.ch/dfr/bv109279.html.

[49] BVerfGE 141, 220 (278) – BKAG

[50] BVerfGE 80, 367 (374) – Diary [Tagebuch] = www.servat.unibe.ch/dfr/bv080367.html.

V. Conclusion

There are three results from this comparative enquiry into the privacy and data protection in the United States and Europe.

First, the law in America grants privacy and data protection in a highly specific way rather than a generalized one. This does not necessarily mean a decreased intensity of protection in all cases. For privacy and data protection based on the Federal Constitution, however, the rule based approach by the U.S. Supreme Court leads to a rather limited protective scope. While Europe acknowledges a general constitutional right to privacy and data protection, the constitutional interpretation in America is focused on certain islands of protection derived from different Amendments.

As a second observation, the rule based approach in U.S. constitutional law results in an all-or-nothing application of the law that entails a certain rigidity. Once a rule like the *third party doctrine* has been established, it is indiscriminately applied to all cases even if new technologies like personal computing or internet communication require a new sensitivity and deserve exceptional rules. The principle based approach in Europe, due to its ubiquitous use of balancing, can more easily adapt to new cases and contexts.

As a third and final result, the Constitutional Courts in Europe, by using the principle based approached to constitutional rights, are tightly controlling the legislative branch. They pursue this control even to the extent that they hand out detailed directives about unwritten legal rights to have data use limited, data erased or generally to be "forgotten". This kind of directive by courts is unknown in the jurisdiction of the U.S. Supreme Court. In America, judicial review is limited by an institutional arrangement where the legislative and administrative branch of government receive a respectful restraint by the courts. This judicial restraint is further facilitated by the rule based approach to constitutional rights. By avoiding balancing and subjecting constitutional claims to a rigid framework of rules and exceptions, the U.S. courts do not take up the task of "optimization". If Europe were to strive for a similar restraint in the courts' jurisdiction, it would have to adapt the principle based approach to a more restricted form.[51]

---

[51] *Axel Tschentscher,* Interpreting Fundamental Rights – Freedom versus Optimization, in: Hermann Pünder/Christian Waldhoff (Hrsg.), Debates in German Public Law, Oxford 2014, at 43 ff. (53 ff.).