UC Law SF International Law Review

Volume 47 | Number 1 Article 2

2-2024

The Origins and Future of International Data Privacy Law

Julian Schneider

The Origins and Future of International Data Privacy Law

JULIAN SCHNEIDER*

Abstract

Data privacy law varies widely across jurisdictions worldwide. Amidst sophistries and jurisdictional conflicts between lawmakers in Europe and the United States, a largely unregulated cross-border data industry emerged, prepared to exploit an unaware or overwhelmed general public. Without governmental support, privacy itself is in grave danger. The people, as true bearers of the fundamental right to privacy, must be put back in control of their data by governments that are aware of their ever-conflicting roles as protectors and aggressors. Scholars like Ari Ezra Waldman, in its book "Industry Unbound," have criticized the common notice and consent approach to privacy as mere performance, calling for more governmental regulation instead of private enforcement. What they often overlook is the international dimension of the issue at hand, the specific and complex history of privacy as a philosophical and legal concept, and the inherent need to ultimately put people in control, not governments.

By recollecting the function and value of privacy, of data, and of corresponding legislation, lawmakers all over the world might be able to enter into a new era of privacy awareness. This article explores possible solutions from an international perspective, based on the historical and philosophical foundations of privacy itself, and a comparison between the privacy history of the United States, Germany, and the European Union.

---

*Julian Schneider is a German attorney and Adjunct Professor of Law at UC Law SF. Due to his multijurisdictional experiences, his main area of practice is international data privacy, with an emphasis on data transfers and cross-border compliance efforts. Besides his German law degree, Julian is a UC Law SF alum (LL.M. '22), holds a CIPP/US certification, and is licensed to practice law in both California and Germany. His research focuses on differences and similarities between legislative approaches to privacy rights.

TABLE OF CONTENTS

I. Introduction 2
II. Data and privacy in law, philosophy, and politics 5
A. Underlying legal conceptions of data 5
B. Philosophical foundations of privacy 8
C. Possible roles of governments 10
III. The story of privacy law so far 12
A. United States: Privacy as absence of governmental intrusion 12
B. Germany: Privacy rights as an integral part of human dignity 16
C. Europe and the EU: Creating a fundamental right to privacy 18
IV. Future law and policy 21
A. United States: In search of a common framework 22
B. European Union: A market for data under the umbrella of fundamental rights 24
C. Germany: Adapting to the GDPR scheme 25
V. Sustainable ways to protect public and individual privacy 27
A. The principle of privacy awareness 28
B. Responsible exercise of individual rights 30
C. Defending public interest 31
VI. Conclusion 32

I. Introduction

Personal data has been framed as "the new oil,"[2] or "the fuel of our future."[3] Unlike oil, however, it is not entirely obvious what kind of machine data would fuel, who is operating the machine, what the destination is, or who should pay the fuel costs. A broad variety of businesses and economies that rely heavily on data usage often operate behind the scenes. Privacy notices and similar means of notification give little, if any, insight into the reality of data processing.[4] Many people feel that something important or potentially dangerous might be happening to their personal information, but without a deeper understanding of what data is and how it is managed, it is

2. *See* Michael Kershner, *Data Isn't The New Oil — Time Is*, FORBES (July 12, 2021, 8:20 AM), https://www.forbes.com/sites/theyec/2021/07/15/data-isnt-the-new-oil—time-is.

3. *Data is the fuel of our future*, XERO BLOG (2015), https://www.xero.com/blog/2016/02/data-fuel-of-our-future/.

4. Rex Chen et al., *Fighting the Fog: Evaluating the Clarity of Privacy Disclosures in the Age of CCPA*, WORKSHOP ON PRIV. IN ELEC. SOC'Y (Nov. 15, 2021), https://doi.org/10.1145/3463676.3485601.

impossible to translate those feelings into actual knowledge. We sometimes call it "Big Data," but few of us can explain the true nature of this invisible force.

The conception of "personal data" does not necessarily invoke a clear picture, nor does the closely related idea of "privacy." While concepts such as "data awareness" are rapidly gaining traction in business environments, there still is a lack of privacy awareness in the general public. This mismatch calls for new approaches.

A quest to identify common international norms in the field of data privacy is prone to fail. There is no commonly accepted idea of privacy, and most countries are still in the process of developing their approaches to personal data. Nevertheless, finding common ground in international data privacy law and creating awareness of existing differences is the purpose of this article. Without an international approach, any meaningful notion of data privacy would be a lost cause. When it comes to data, national borders have no protective function.[5] Thus, people all over the world are similarly affected. Because there is no opt-out of society, there is no opt-out of a global debate on the future of data privacy.

To identify possible international approaches, this article will first analyze the legal, philosophical, and political nature of both data and privacy. This is intended to lay a foundation for further analysis. One of the biggest issues in the privacy context is the ambiguity of its key concepts, the variety of terms, and the ideas that are used to describe a rather vague feeling of intrusion. To understand what personal data might be, and what privacy is intended to be, it is necessary to know where both data and privacy come from, what types of interests might be affected by it, and how, or for what purposes, governments could act in relation to it.

Second, the article will narrate the story of privacy law so far, focusing on the United States and the European Union. Within the European Union, Germany, a trailblazer for modern privacy laws, is offered as one example of a member state in the process of adjusting to European rules. This part will discuss the distinct ways the United States, Europe, and Germany have been, and still are, choosing to balance public and individual privacy interests. This analysis will highlight the values that are at the core of each of their approaches. Thus, this part of the article serves to identify the specific purposes and the roles these three governments have assumed in the past and are assuming now in relation to data.

---

5. There are, of course, some possible exceptions to this rule, due to internet censorship measures that, to various extents, still exist in several countries. However, restricting free access to the internet, albeit potentially effective, would be a rather Kafkaesque way of promoting data privacy.

The third part of the article will analyze interrelations between privacy law traditions and the current data privacy legislation of these three governmental entities to predict future developments. Briefly touching on data ownership, the article will assess the compatibility of contemporary concepts in data privacy with these governments' respective historical approaches, and it will also identify the values underlying these approaches. In other words, in this part the article will discuss reasons why nations and supranational entities, in their respective legal traditions, might choose to favor certain approaches over others, and it will identify the possible consequences in the field of data privacy law.

Last, based on the results of this assessment, the article will propose several concepts to sustainably protect public and individual privacy interests in the age of "Big Data." After analyzing how governments in general can act in the field of data privacy, have been acting in the past, are acting in the present, and might act in near future, this final part answers the question: How *should* governments act to preserve, protect, and promote crucial concepts of privacy in general, and data privacy in particular?

Because there is no generally established language of data privacy, this article, where necessary, will use the comprehensive and, for the most part, clearly defined, General Data Protection Regulation (GDPR)[6] terminology to avoid ambiguities. Therefore, as an example, an individual whose data is concerned by a certain action will be referred to as "data subject,"[7] and the entity determining the purposes and means of data processing will be referred to as "controller."[8] This is not to say that the GDPR choice of words should generally determine notions in the field of data privacy, but it does at least provide a set of basic definitions that are easily accessed.[9]

---

6. Regulation 2016/679 of The European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, 2016 O.J. (L 119) 1 [hereinafter GDPR].

7. *See id.* art. 4(1). The choice of this term is particularly intriguing. In its official German version, the GDPR term is "betroffene Person," or "affected person." Unlike the English word "subject," the German word "Subjekt" does have a secondary, commonly used meaning that originates in German idealism and refers to a conscious entity in relationship with a certain object. A subject in this sense is the acting part of this relationship, while the object is the part affected by the actions of the subject. This different understanding and the corresponding choice of words might reveal more than intended about the current state of data privacy. Without anticipating too much, the assessment might be correct that, under the GDPR and any other privacy law, the subject is anything but an acting part of a data privacy relationship.

8. *See id,* art. 4(7).

9. It would arguably be a valid option to use the CCPA terminology instead. However, as the CCPA, albeit broader than most existing U.S. law, still refers to "consumers" and "businesses," the GDPR provides for a broader range of possible situations.

II. Data and privacy in law, philosophy, and politics

Data privacy law is more than just another application of privacy law, and even general notions of privacy law vary widely. While personal data is the subject of modern economic and legal scholarship, the concept of privacy has a colorful history. Privacy has frequently been described as an essential part of human culture. It is a philosophical idea that was, for good reason, transferred to a legal context long after its creation.

Personal data, on the other hand, emerged in a potentially business-oriented context. Quantified knowledge about certain circumstances of existence has never been deemed essential for existence itself because philosophers, as scholars of existence, emphasize cognitive abilities rather than our physical presence as humans in the world that surrounds us.[10] The results of these cognitive abilities and processes, of thinking, asking, and doubting, are of qualitative rather than quantitative nature. Accordingly, quantitative dimensions of our existence have traditionally been of lesser interest for modern philosophy but can give insight into human habits and needs.

Due to this fact, personal data is largely defined by its economic value. To handle and to define economic assets is a traditional field of legal scholarship. This is arguably not the case for defining essential notions of humanity, a field in which other branches of knowledge, such as philosophy or even theology, used to prevail.

A. Underlying legal conceptions of data

The mere fact that much legal scholarship on data exists does not necessarily create any degree of clarity. One fact, however, is undisputed: personal data does have both a non-economic value for the person it belongs or relates to, and a potential economic value for third parties it does not belong or relate to. Those values are necessarily conflicting. The non-economic value of data is defined by the data subject's privacy interests, while the economic value necessarily requires a certain degree of interference with those interests.

Thus, the value of data, as an important factor for determining its legal nature, is highly subjective and highly exclusive. Personal data can be a marketable good and an integral part of a person at the same time. Because

10. *See* RENÉ DESCARTES, *The Principles of Philosophy*, *in* 1 THE PHILOSOPHICAL WORKS OF DESCARTES (Cambridge Univ. Press 1911) (1644).

there usually is no (lawful) market for integral parts of persons, this circumstance alone can be worrying.

Other features distinguish personal data from other established legal concepts. Unlike personal property, data is not tangible. Unlike intellectual property, most data is not created intentionally.[11] Personal data is an intangible byproduct of human conduct that has value for those who collect and analyze it. As such, data resembles scientific facts, or news reports. However, the most valuable aspect of personal data is not merely the information contained, but the fact that an individual, or some group of individuals, behaves in a way that can be inferred from the data. Personal data, unlike scientific facts or news, can never fully be severed from its origin.

As such, personal data is an unusual phenomenon. Nonetheless, legal scholars have been proposing a broad variety of approaches to handle it by fitting data into well-established legal categories. The aforementioned legal concepts, especially those that are related to property and ownership, are the most common. However, even the most zealous data ownership advocates concede that neither is a perfect solution.[12] Even if data could be painstakingly fitted into a traditional concept of personal or intellectual property, it would not work in all jurisdictions' permutations of those concepts.[13] Therefore, there are some arguments for treating data as the new category of rights it seems to be.

Regarding the three different jurisdictions this article examines, there is no clear standard either.

The GDPR definition merely defines data by referring to it as "information," which is not particularly helpful in determining its legal nature.[14] Conversely, this means that the GDPR framework is intended to function regardless of the legal nature data may have in any of the European Union's member states, or any other country.

Germany, one of these member states, is a traditional civil law jurisdiction. As such, its laws provide definitions of related legal concepts that clearly exclude data, for example: "Only corporeal objects are things as

11. Intentional creation, for most jurisdictions, is the main reason to protect intellectual property. *See* Berne Convention for the Protection of Literary and Artistic Works art. 2(1), Sep. 9, 1886, 102 Stat. 2853, 1161 U.N.T.S. 3.

12. *See, e.g.*, Jeffrey Ritter &Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. REV. 220, 227 (2017-2018).

13. Additionally, there are major differences between common law and civil law jurisdictions. Common law tends to be more flexible in allowing entirely new forms of intangible property or intangible assets like goodwill, while many civil law jurisdictions have clear statutory or even constitutional definitions they would need to amend.

14. GDPR, *supra* note 5, art. 4(1).

defined by law,"[15] or for works protected as intellectual property: "Only the author's own intellectual creations constitute works within the meaning of this Act."[16] Data is neither a corporeal object[17] nor an intellectual creation.[18] Therefore, data does not lie within the scope of ownership or similar rights in Germany.

U.S. courts so far have refrained from defining data as a concept, or from explaining its legal nature.[19] However, merely because there is law on personal data, it is evident that data exists from a legal perspective in the United States. The Supreme Court held in *Int'l News Serv. v. AP* that publicly available information can be, to some degree, affected by property rights, if such information is obtained "as the result of organization and the expenditure of labor, skill, and money."[20] In this case, the news agency Associated Press (AP) was awarded a quasi-property right in the results of its enterprise to gather news from other sources. Accordingly, its rival, International News Service, violated this right by obtaining news through early publications of AP's members and selling the news to other media outlets. This conception of effort-based quasi-property rights might be of importance for disputes among controllers of data (because they expend labor, skill, and money to obtain information), but it does not help determine the legal nature of data for the data subject who effortlessly generates data without even intending to do so.

Another famous property rights case, *Moore v. Regents of the Univ. of Cal.*, examined property rights in bodily cells that were taken as samples by doctors and later used for medical research. The case suggests "that it cannot be said that a person has no property right in materials which were once part

15. BÜRGERLICHES GESETZBUCH [BGB] [Civil Code], § 90 (Ger.), translation at http://www.gesetze-im-internet.de/englisch_bgb/index.html.

16. URHEBERRECHTSGESETZ [UrhG] [Copyright Act], Sept. 9, 1965, § 2 para. 2 (Ger.), translation at https://www.gesetze-im-internet.de/englisch_urhg/englisch_urhg.html.

17. Regardless of its storage location, data itself never can be touched. The fact that something can be stored on a corporeal object is not determinative for its legal nature. However, data embodied in a storage medium can be corporeal as such. This does not determine the legal nature of the stored data itself but rather the legal nature of the specific data in the specific way it is stored on the medium. Basically, the corporeality of the storage medium is transferred to the data stored but not to data as such. Bundesgerichtshof [BGH] [Federal Court of Justice] Oct. 13, 2015, 207 ENTSCHEIDUNGEN DES BUNDESGERICHTSHOFS IN ZIVILSACHEN [BGHZ] 163 (Ger.), touches this complicated topic.

18. Some data might possibly be an intellectual creation as well. However, this would not make this data intellectual property just for being personal data. Instead, in such cases, the underlying intellectual creation would be protected as such, while the data it includes merely is protected in its function to be part of a creation.

19. The same is true for the terms "personal information," or "personally identifiable information."

20. Int'l News Serv. v. Associated Press, 248 U.S. 215, 240 (1918).

of his body."[21] This rather cryptic assessment of property rights in bodily cells, or the "non-absence" of such rights, as the court puts it, raises an issue that is similar to the legal nature of personal data. Bodily cells are "generated" as effortlessly as data and are inherently connected to the individual who "generated" them. On the other hand, as much as *Int'l News Serv.* relates to intangible information of general interest, *Moore* concerns tangible things that typically are kept in private. Personal data is somewhere in between, and it therefore must be assumed that the distinguishing features of these cases, expenditures in *Int'l News Serv.*, and tangibility in *Moore*, are determinative for the existence of property interests. Neither case can be applied to data without creating new problems.

Data therefore has no apparent legal nature. Especially in the U.S., the concept of data ownership still encounters both encouragement[22] and well-founded criticism.[23]

Although there are some legal concepts that might play a role in analyzing different ideas of data privacy, none of them provides an ultimate definition of personal data. The question remains, however, whether such a definition is necessary to adequately protect personal data. There are a variety of established legal concepts and individual rights, like freedom of speech or human dignity, that apparently do not require legal categorization to be effectively protected. Discussions of "free speech ownership" or "dignity ownership" are unheard of. Of course, there are reasons why data should be handled differently. Therefore, this article revisits this question after analyzing how personal data fits into the big picture of individual rights protection.

Because the definitions of personal data and privacy are inextricably intertwined, a closer look at ideas of privacy itself might be helpful at this point.

B. Philosophical foundations of privacy

Privacy is not a creation of legal scholarship but an established sphere of human existence the law attempts to protect. As such, it is not necessary (and would in fact be harmful) to legally define the individual interests

21. Moore v. Regents of the Univ. of Cal., 215 Cal. App. 3d 709, 249 Cal. Rptr. 494, 505 (1988).

22. *See, e.g.*, Jurcys, Paulius et al., *Ownership of User-Held Data: Why Property Law is the Right Approach*, JOLT DIGEST (Sept. 21, 2021), https://jolt.law.harvard.edu/digest/ownership-of-user-held-data-why-property-law-is-the-right-approach.

23. *See, e.g.*, Lothar Determann, *No One Owns Data*, 70 HASTINGS L.J. 1, 1 (2018).

privacy may include. What exactly is within the scope of privacy interests must be resolved on a case-by-case basis. Thus, privacy law focuses on ways to balance and to protect individual interests instead of defining them. Exploring the content of the protected sphere of privacy is subject to other approaches.

Accordingly, in their groundbreaking article "The Right to Privacy," the founding fathers of American privacy law, Louis D. Brandeis and Samuel D. Warren, are not trying to list interests that are possibly protected by a right to privacy. Instead, Warren and Brandeis emphasize the role of legal concepts in protecting individual and social demands for privacy.[24] However, these demands for privacy originate elsewhere. Possibly inherent in human nature, the right to be left alone – first formulated by Aristotle – is considered a basic human need.[25] For centuries, this concept was largely illusory for, and inaccessible to, most commoners. If privacy existed at all, it was a privilege of the well situated. Ancient societies, until relatively recently, were not able and often not willing to provide their members with sufficient physical or mental space to establish a general right to privacy.[26]

The rise of the bourgeoisie, finding support in the philosophy of Enlightenment,[27] abruptly turned this upper-class privilege into a core principle of civic self-awareness, making the age of enlightenment an age of privacy. In an urban society, previously unknown needs for intellectual and physical distancing developed. Thus, Aristotle's ideas finally found broad application and were further developed by philosophers of the time like John Stuart Mill.[28]

Nowadays, that there is a right to privacy is largely undisputed.[29] Modern philosophers like John Rawls consider a sphere of individual liberty

---

24. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

25. JUDITH A. SWANSON, THE PUBLIC AND THE PRIVATE IN ARISTOTLE'S POLITICAL PHILOSOPHY (Cornell Univ. Press 1992) provides a comprehensive overview of Aristotle's public and private spheres.

26. A HISTORY OF PRIVATE LIFE, VOL. I-III explores historical limitations of privacy in great detail. *See* PAUL VEYNE ET AL., 1 A HISTORY OF PRIVATE LIFE (Paul Vayne et al. eds., Harvard Univ. Press 1992); GEORGES DUBY ET AL., 2 A HISTORY OF PRIVATE LIFE (Georges Duby et al. eds., Harvard Univ. Press 1993); ROGER CHARTIER ET AL., 3 A HISTORY OF PRIVATE LIFE (Roger Chartier et al. eds., Harvard Univ. Press 1993).

27. *See, e.g.*, JOHN LOCKE, TWO TREATISES OF GOVERNMENT 116 (The Staff of Thomas Tegg ed., 1823) (1690) . Notably, Locke here describes a right of property in the own person.

28. *See* JOHN STUART MILL, ON LIBERTY 24, 167 (The Walter Scott Publishing Co., Ltd ed., 1901) (1859).

29. The main philosophical critiques aim at the ambiguous definitions of privacy. *See, e.g.*, Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393 (1977). Apart from that, even the originalist criticism towards a constitutional right to privacy does not deny the

– that necessarily includes privacy – the core value of any societal, and therefore legal, framework.[30] The basic idea of modern fundamental rights is that there needs to be some form of an individual safe space, designed to exclude governmental actors and other parties.[31]

Data privacy, and modern privacy law in general, therefore can be described as the attempt to transfer the age of privacy's core values, the civic self-awareness that originated in the 19th century, into the age of data. Data, in this formulation, is the main currency of the 21st century information-based economy. How to approach this ambitious transfer project is a question of governance.

C. Possible roles of governments

An age of privacy violations closely followed this first age of privacy. Totalitarian governmental systems of different shades, like the USSR or Nazi Germany, did not accept any idea of privacy, because anything that did not happen in plain view was considered a potential danger for their rulers. Totalitarianism, by its nature, strives for complete control of every single citizen. To exercise complete control, it is necessary to know what any part of society, and consequentially every single citizen, is doing at any given time.[32] Complete control requires complete knowledge, and any form of privacy interest therefore constitutes an obstacle. A whole genre of dystopian literature was inspired by such governments and their ways of intrusion.[33]

---

existence of a more general, non-constitutional right to privacy. Griswold v. Connecticut, 381 U.S. 479, 508 (1965).

30. The "First Principle" of justice, according to Rawls, is that "[e]ach person is to have an equal right to the most extensive total system of equal basic liberties compatible with a similar system of liberty for all." JOHN RAWLS, A THEORY OF JUSTICE 266 (Harvard Univ. Press rev. ed. 1999) (1971).

31. *See* Julie E. Cohen, *How (Not) to Write a Privacy Law*, 21-02 KNIGHT FIRST AMEND. INST. (Mar. 23, 2021), https://knightcolumbia.org/content/how-not-to-write-a-privacy-law.

32. The philosophical mastermind of Nazi totalitarianism in Germany during the 1930s, Carl Schmitt, described a "total state, which potentially embraces every domain. This results in the identity of state and society." CARL SCHMITT, THE CONCEPT OF THE POLITICAL 22 (The Univ. of Chicago Press ed. 2007) (1927).

33. Apart from the most prominent example, 1984 by George Orwell, FAHRENHEIT 451 by Ray Bradbury, and BRAVE NEW WORLD by Aldous Huxley also originated in this period. However, as ATLAS SHRUGGED by Ayn Rand famously shows, there were quite different dystopian views even in an era dominated by experiences of totalitarian regimes. Because a comparison of those dystopian visions would go far beyond the scope of this note, it is fortunate that Neil Postman already made such an attempt. *See* NEIL POSTMAN, AMUSING OURSELVES TO DEATH AT XIX-XX (Penguin Group ed. 2006) (1985).

Even democratic governments have never been entirely free of suspicion against individual privacy interests, however. The National Security Agency (NSA) surveillance disclosures may serve as a reminder.[34] On the other hand, modern democratic governments dedicate themselves to the protection of their citizens' privacy interests. Transgressions aside, there are four main functions a democratic government may have in relation to individual privacy interests: the intruder, the watchdog, the regulator, and the gatekeeper.

First, governments are intruders. They are notorious trespassers in the land of privacy. In many cases, such trespass will be justified. Issuing a passport or collecting taxes, for example, are perfectly legitimate, although not necessarily pleasant, reasons to collect a variety of data. The same can be true for law enforcement purposes.[35] Furthermore, even if they could be criticized, there are legitimate intelligence interests in protecting the nation and its citizens. Gathering data is an important, albeit inherently conflict-laden, part of this work.[36]

Governments are watchdogs. By establishing regulatory agencies, enforcing penalties, enacting security standards and protocols, and regulating private action, a government can ensure that nobody gains unlawful access to data. The duties of governmental watchdogs can also be delegated, for example, by legally requiring private entities to accept supervision.[37]

The governmental function as regulators in a narrow sense is similar and closely connected to their role as watchdogs. Regulatory functions in a narrow sense concern the way in which private and public entities conduct their lawful access to and processing of data. In this role, governments route the stream of data instead of merely regulating access to it.[38]

---

34. *See* Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN (June 6, 2013, 6:05 AM), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

35. The legitimacy of governmental action that is connected to such basic state functions usually is assumed, at least in the United States, as a precondition of privacy legislation. *See, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552a. As discussed below, the GDPR requires a justification even in case of basic governmental functions. However, at least if the Fourth Amendment is concerned, which will often be the case in law enforcement, "the ultimate touchstone . . . is 'reasonableness.'" Riley v. California, 573 U.S. 373, 381 (quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006)). Therefore, at least for the purposes of law enforcement, there will be some kind of balancing tests under each framework.

36. *See, e.g.*, 50 U.S.C. § 1802.

37. *See, e.g.*, GDPR, *supra* note 5, art. 37.

38. *See, e.g.*, *id.* art. 44.

Last, governments can be gatekeepers. They can provide access to personal data for data subjects and sometimes for others. Under certain circumstances, there might be a third-party interest in personal data the third party is not able to obtain but has a right to. For example, this need might arise in case of a car accident, when a victim needs to access insurance information of a liable party. Whether this data is controlled by the government or by a private entity, objective courts or agencies can ensure that the claim is valid, and that the claimant should gain access.[39]

Those roles may be conflicting in some instances. Trespassers are bad watchdogs, and someone keeping a gate might wrongfully decide to open it for their own purposes. In other words, the question of *Quis custodiet ipsos custodes?*[40] must be considered to address possible conflicts of interest. In many cases, however, ordinary governmental checks and balances will suffice.

While the main functions or roles of governments in the privacy context are now recognized all over the world, this does not mean that any consensus would exist with regard to practical consequences.

III. The story of privacy law so far

The history of privacy law is fractured. Despite the long history of privacy as a philosophical concept, political attempts to convert it into an enforceable right only began to appear in the 19th century.

A. United States: Privacy as absence of governmental intrusion

As one of the oldest constitutions in force in the world, the Constitution of the United States, unsurprisingly, is silent on several issues that other jurisdictions have later decided to regulate on a constitutional level. Several U.S. state constitutions do provide protections for privacy rights that the federal Constitution does not offer on its face.[41]

---

39. *See, e.g.*, UrhG § 101 para. 9 (Ger.).

40. Latin saying, "Who will guard the guards themselves?"

41. Alaska, ALASKA CONST. art. I, § 22, Arizona, ARIZ. CONST. Art. II, § 8, California, CAL. CONST, Art. I § 1, Florida, FLA. CONST. Art. I, § 23, Hawaii, HAW CONST. Art. I, § 6, Illinois, ILL. CONST., Art. I, § 6, Louisiana, LA. CONST. Art. I, § 5, Montana, MONT. CONST., Art. II § 10, New Hampshire, N.H. CONST. PT. FIRST, Art. 2-b, and South Carolina, S.C. CONST. ANN. Art. I, § 10, explicitly protect "privacy" in their constitutions. Washington provides a quite similar right not to be disturbed in private affairs. WASH. CONST. Art. I, § 7. Additionally, there are constitutional provisions that extend protection from unreasonable searches to electronic data, in Michigan, MICH. CONST. Art. I, § 11, and Missouri, MO. CONST.

As mentioned, Brandeis and Warren's article "The Right to Privacy" is widely considered the first in-depth approach to defining the scope of constitutional privacy rights. However, this piece of scholarship did not have an immediate legal effect at the federal level because it mainly focused on tort law, an area the States traditionally handle.[42] Instead, a large part of the Supreme Court's early privacy precedent is found in an entirely different area of law: the Court's Fourth Amendment jurisprudence.[43]

The Fourth Amendment provides a broad scope of protection for citizens against governmental searches and seizures, especially by requiring a warrant.[44] However, this requirement only applies to actions that are considered searches and seizures. In earlier days, the courts defined searches and seizures by applying traditional common law rules to the categories of items that are explicitly mentioned in the Constitution.[45] Not surprisingly, the most powerful dissenter to such opinions was then-Justice Brandeis.[46] As a key Brandeis dissent stated almost a century ago, scientific advances "may bring means of exploring unexpressed beliefs, thoughts and emotions."[47]

Accordingly, during the 1960s and in light of some of those scientific advances, the U.S. Supreme Court decided to fundamentally change its course towards a privacy-oriented test that turns on the reasonableness of a subjectively held expectation of privacy to determine whether a search occurred.[48] In other words, privacy expectations of society in general play a vital role in determining whether individuals may reasonably expect privacy under the circumstances of the case at hand. Because of that, society's privacy standards have frequently been discussed in Fourth Amendment cases.[49]

Art. I, § 15. These approaches to constitutional privacy rights deserve to be mentioned here; however, this note focuses on federal law.

42. U. S. CONST. art. I § 8 does not grant a general power on the field of tort law. Therefore, most of it is left to the states. There are, however, some federal torts connected to Congress's powers, 42 U.S.C. § 1983 being the most noteworthy.

43. Katz v. United States, 389 U.S. 347 (1967). *But see* Griswold v. Connecticut, 381 U.S. 479 (1965).

44. U. S. CONST. amend. IV.

45. Olmstead v. United States, 277 U.S. 438, 488 (1928) (citing Carroll v. United States, 267 U.S. 132, 149 (1923)).

46. , *Id.* at 471-85.

47. *Id.* at 474.

48. Katz v. United States, 389 U.S. 347, 361 (1967). Even if seemingly applied by the majority, Justice Harlan provides the test in his concurrence.

49. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 744 (1979) (no reasonable expectation of privacy in numbers dialed from a phone); Bond v. United States, 529 U.S. 334, 338-39 (2000) (reasonable expectation of privacy in contents of luggage placed in an overhead bin of a bus); Riley v. California, 573 U.S. 373, 392 (2014) (reasonable expectation of privacy in data stored

Thus, federalism has played an important role in the development of U.S. privacy law. While Fourth Amendment jurisprudence typically limits governmental intrusion, it is the area of tort law that often defines personal boundaries and grants governmental protection. By allocating most privacy tort cases to state court systems, federalism largely limited Supreme Court privacy precedent to Fourth Amendment questions. As a result, the history of federal U.S. privacy law largely is a history of governmental intrusion and its justification: whether certain types of conduct reasonably justify an expectation of privacy against the government or not.

Other federal privacy laws do not provide a comprehensive scheme in general but do provide protections for some specific sectors.[50] The U.S. Privacy Act of 1974,[51] which establishes a system of fair information principles, is arguably the most comprehensive of these statutes, at least in theory.[52] But there are also federal laws that are considered a danger for privacy interests. In particular, the USA PATRIOT Act,[53] amended by the USA FREEDOM Act,[54] provides the government with a variety of legal tools that can, and are supposed to, be used for mass surveillance.

The existence of such abundant governmental powers to gather data of individuals was a main reason the European Court of Justice (ECJ) expressed its doubts about whether the U.S. "ensures an adequate level of protection" for personal data of EU citizens.[55] Eventually, the level of possible privacy invasions by the U.S. federal government resulted in two landmark

---

on a mobile phone); United States v. Knotts, 460 U.S. 276, 281 (1983) (no reasonable expectation of privacy in movements of a car on public roads); United States v. Karo, 468 U.S. 705, 714 (1984) (reasonable expectation of privacy in movements of an item in a private residence); Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (reasonable expectation of privacy in the wholeness of public movements of an individual).

50. The Children's Online Privacy Protection Rule [COPPA], the Fair Credit Reporting Act [FCRA], the Gramm-Leach-Bliley Act [GLBA], and the Health Insurance Portability and Accountability Act [HIPAA] are noteworthy federal regulations of specific fields.

51. Privacy Act of 1974, 5 U.S.C. § 552a.

52. The Privacy Act only applies to collection of US citizen or lawful permanent resident data by federal agencies. 5 U.S.C. § 552a(a)(2). Thus, albeit seemingly broad in its protections and not limited to a specific field in the sense of an area of data collection, the actual significance of the act is rather limited.

53. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, H.R. Res. 3162, 107th Cong. (2001) (enacted).

54. Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring (USA FREEDOM) Act of 2015, H.R. Res. 2048, 114th Cong. (2015) (enacted).

55. This level of protection is a statutory requirement for data transfers to third countries, if based on an adequacy decision issued by the Commission. GDPR, *supra* note 5, art. 45(1).

decisions[56] of the ECJ (Schrems I and Schrems II) suspending adequacy decisions under the Safe Harbor Agreement in 2015[57] and, following the enactment of the GDPR, under the Privacy Shield Agreement in 2020.[58] Both Schrems I and Schrems II refer to U.S. legislation and Presidential directives that endanger privacy interests of European citizens, and clearly establish that there generally are conflicting views of privacy rights between the U.S. and the European Union.[59]

More recent events put this conflict in a nutshell. Shortly before President Biden and Ursula von der Leyen, President of the European Commission, agreed on a new adequacy agreement that will replace the suspended Safe Harbor and Privacy Shield,[60] the U.S. Supreme Court published an opinion that extends the scope of state secrets privileges, likely increasing the hurdles for challenging governmental surveillance activities in U.S. courts.[61] In this case, *FBI v. Fazaga*, the Court held that Section 1806(f) of the Foreign Intelligence Surveillance Act (FISA) does not override the state secrets privilege. As a result, privacy-related litigation under FISA will be impossible if it is deemed a threat to national security by a privilege-holder, such as the FBI.

This episode illustrates the role governmental intrusion has been playing in the U.S. debate on data privacy. There is an ongoing conflict that is fueled not only by a lack of legal protection at federal level in the United States, but also by a high governmental interest in data. Therefore, it is difficult to imagine the U.S. government assuming a lead role in protecting privacy at this point. However, data privacy is a dynamic area of law. With growing public awareness and concern, the U.S. might rebalance its efforts towards a more regulatory function. To some extent, this will also be

---

56. Alex Hern, *The background to EU citizens' court win over US tech giants*, THE GUARDIAN (July 16, 2020), https://www.theguardian.com/technology/2020/jul/16/the-background-to-eu-citizens-court-win-over-us-tech-giants gives an overview.

57. Case C-362/14, Maximilian Schrems v. Data Prot. Comm'r, 2015, E.C.J., https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=996140 (Oct. 6, 2015) [Schrems I].

58. Case C-311/18, Maximilian Schrems v. Data Prot. Comm'r, 2019, E.C.J., https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=996140 (July 16, 2020) [Schrems II].

59. Because the scope of the decisions was limited to effects on EU citizen and their data, the Schrems II court focused on the Foreign Intelligence Surveillance Act which was amended by the PATRIOT Act as well.

60. European Commission, *Statement by President von der Leyen with US President Biden* (Mar. 25, 2022), https://ec.europa.eu/commission/presscorner/detail/en/statement_22_2043.

61. FBI v. Fazaga, 142 S. Ct. 1051, 1053 (2022).

necessary to satisfy European courts, thereby ensuring compliance with GDPR data transfer requirements.

B. Germany: Privacy rights as an integral part of human dignity

The German constitution[62] has a special history. It serves as an example of a more recent constitution, ratified after World War II. Drafted in the shadow of the Nazi era and its inconceivable crimes, the key principle of this new constitution is to be found at its beginning: "Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority."[63] Thus, human dignity is the ultimate touchstone of governmental action in Germany. Other fundamental rights, like the free development of personality,[64] merely serve to promote this core principle.

The German constitution does not include an explicit right to privacy. Shortly after its enactment, however, the Federal Court of Justice made clear that a general right to all aspects of personality is implied in both human dignity and the right to free development of personality.[65] In later decisions, the German Constitutional Court largely agreed.[66]

One important, more specific part of this general right of personality, is the right to informational self-determination the Constitutional Court established in its landmark "census verdict" of 1983 that explicitly targets data processing practices.[67] In that case, many German citizens filed a complaint against a newly enacted law that aimed to perform a census. The Constitutional Court invalidated the law and held that the concept of human dignity includes a right to limit data processing, and that this right can be violated by overbroad data collection. Thus, the German right to privacy is directly traceable to, and inseparably intertwined with, the concept of human dignity. Like the Fourth Amendment to the U.S. Constitution, its German analogue affects governmental action, such as searches conducted by police officers.[68]

---

62. GRUNDGESETZ [GG] [Basic Law], May 1949, translation at http://www.gesetze-im-internet.de/englisch_gg/index.html.

63. *Id.* at art. 1, para. 1.

64. *Id.* at art. 2, para. 1.

65. BGH, May 25, 1954, 13 BGHZ 334, 338.

66. Bundesverfassungsgericht [BverfG] [Federal Constitutional Court] June 5, 1973, 35 ENTSCHEIDUNGEN DES BUNDESVERFASSUNGSGERICHTS [BverfGE] 202, 219 (Ger.).

67. BverfG, Dec. 15, 1983, 65 BverfGE 1-71.

68. Such police action has additional statutory limits that predate the "census verdict". *See, e.g.*, STRAFPROZESSORDNUNG [StPO] [Code of Criminal Procedure], §§ 102-110, translation at https://www.gesetze-im-internet.de/englisch_stpo/ (Eng.). Similar to the Fourth

Notably, German constitutional rights do not only bind the government in its actions. As a system of values, fundamental rights may also apply to individual citizens through the doctrine of indirect third-party effects.[69] This doctrine applies to so-called "gateway clauses" that can, for example, be found in statutory torts law and require additional interpretation. This area of law makes frequent use of indeterminate legal terms like "public policy,"[70] "another right,"[71] or the concept of "good faith."[72] To determine the scope of such terms in private law relationships, German courts therefore will use the terms as a "gateway" to consult the constitution and provide protection against any unjustified violations of privacy, even if not committed by the government. As a result, there is a strong emphasis on the German courts' role as watchdogs not only for the remaining branches of government, but also between private parties.

Connected to the latter role, German courts also have a gate-keeping function. There are several statutes that give third parties the right to access data, provided a court allows them to do so. The Freedom of Information Act[73] applies to public records, while the Telecommunications Telemedia Data Protection Act regulates the field of inventory data stored by private entities.[74]

In 1977, likely affected by mass surveillance conducted by the totalitarian government of East Germany, West Germany enacted its first comprehensive data privacy law on federal level, one of the first comprehensive data privacy laws worldwide.[75] This statute underwent several substantial changes in the aftermath of the 1983 "census verdict" that

Amendment, many of these statutory limits, like the warrant requirement, already were part of the REICHSSTRAFPROZESSORDNUNG of 1877, the earliest direct predecessor of the federal Code of Criminal Procedure.

69. BverfG, Jan. 15, 1958, 7 BverfGE 198, 208.

70. Bürgerliches Gesetzbuch [BGB] [Civil Code] § 826, translation at http://www.gesetze-im-internet.de/englisch_bgb/index.html.

71. *Id.* at § 823, para. 1.

72. *Id.* at § 242.

73. GESETZ ZUR REGELUNG DES ZUGANGS ZU INFORMATIONEN DES BUNDES [IFG] [Freedom of Information Act], Sep. 5, 2005, translation at https://www.gesetze-im-internet.de/englisch_ifg/.

74. TELEKOMMUNIKATIONS-TELEMEDIEN-DATENSCHUTZ-GESETZ [TTDSG], Dec. 1, 2021, no official translation available. § 22(3) establishes proceedings to access such data concerning third-party data subjects.

75. BUNDESDATENSCHUTZGESETZ [BDSG] [Federal Data Protection Act], Jun. 30, 2017, translation at https://www.gesetze-im-internet.de/englisch_bdsg/.

required the government to limit and justify its data collection.[76] In 2001, another comprehensive amendment followed to comply with European standards.[77] Eventually, in 2017, the parliament amended the Federal Data Protection Act to ensure its compatibility with the GDPR.[78]

According to the Constitutional Court's jurisprudence, German privacy right traditions remain relevant notwithstanding common European regulations. As the Constitutional Court held in its "As Long As" decisions,[79] the Constitutional Court will defer towards European legislation and jurisdiction as long as the European Union maintains to provide a protection of fundamental rights that is essentially comparable to German constitutional standards.

Thus, even the GDPR will not entirely sever traditional German notions of privacy law from its constitutional roots. German courts and governmental agencies have continually been assuming their role as privacy watchdogs, and this is viewed as their historical, constitutional duty.

C. Europe and the EU: Creating a fundamental right to privacy

As a result of ongoing political struggles, there is no constitution of the European Union.[80] However, in 2009, the member states ratified a document (the Treaty of Lisbon) that included the main ideas of the failed Treaty establishing a Constitution for Europe.[81] Part of the Treaty of Lisbon was the Charter of Fundamental Rights of the European Union,[82] which is the main legal source of human rights on EU level.

---

76. Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes [Law for the Further Development of Data Processing and Data Protection], Dec. 20, 1990, BGBl I at 2954.

77. Gesetz zur . . .nderung des Bundesdatenschutzgesetzes und anderer Gesetze [Law amending the Federal Data Protection Act and other laws], May 18, 2001, BGBl I at 904.

78. Gesetz zur Anpassung des Datenschutzrechts [Act to Adapt Data Protection Law], June 30, 2017, BGBl I at 2097.

79. BverfG, 73 BverfGE, Oct. 22, 1986, 339, 340. "As long as," the colloquial name of the decision, refers to the formula that the Constitutional Court will refrain from intervening "as long as" the European Union will maintain the mentioned standards.

80. The Treaty Establishing a Constitution for Europe, Rome, Oct. 29, 2004, 2004 O.J. (C310) 1, never entered into force. It remained unratified due to referendums in France and the Netherlands that rejected the treaty after heated discussions in most European countries. As of today, this was the last attempt to establish a constitution for the European Union.

81. Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Dec. 13, 2007, 2007 O.J. (C306) 1 [hereinafter Treaty of Lisbon].

82. Charter of Fundamental Rights of the European Union of Mar. 30, 2010, 2010 O.J. (C 83) 389.

An observer of European politics might assume that its main purpose is to create confusion. This assumption gains support when one considers the Charter of Fundamental Rights and its history. The Charter is largely based on the European Convention on Human Rights, drafted in 1950 by the Council of Europe.[83] Unlike the European Council or the Council of the European Union, the Council of Europe is not a body of the European Union but a separate entity.[84] Thus, for purposes of this article, Europe's constitutional or quasi-constitutional history of privacy law begins in 2009 with the Treaty of Lisbon, even if it has similarities with other documents that have similar names and were enacted by similarly sounding but entirely different entities.[85]

There are, however, much earlier traces of privacy legislation in Europe. During the 1970s and spurred by emerging computing technology, the European Parliament repeatedly urged the Commission to act in the field of data privacy.[86] These exhortations eventually resulted in enactment of a GDPR predecessor,[87] the Data Protection Directive. The Directive was revolutionary in its way but shared the flaws of other EU directives.

Directives are legal acts that require member states to achieve a certain result but do not prescribe "the choice of form and methods" to achieve it.[88] Leaving this choice to member states sometimes can be advantageous due to specific legal, cultural, or other traditions.[89] In other cases it merely leads to fragmentation and confusion about applicable legal standards. The regulation of data streams is not bound by national borders, and there are no specific cultural traditions in handling personal data among the member

83. Eur. Consult. Ass.,European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14 (1950).

84. Eur. Consult. Ass., Statute of the Council of Europe, London (1949).

85. Unless indicated otherwise, "Europe" henceforth refers to the European Union and its member states to minimize the mentioned confusion.

86. *See, e.g.*, Parliament Resolution on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing of Mar. 13, 1975, 1975 O.J. (C60) 48; Parliament Resolution on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing of Apr. 8, 1976, 1976 O.J. (C100) 27.

87. Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data of Nov. 23, 1995, 1995 O.J. (L281) 31 [hereinafter Data Protection Directive].

88. Consolidated Version of the Treaty on the Functioning of the European Union of Oct. 26, 2012, 2012 O.J. (C326) 1, art. 288 [hereinafter TFEU].

89. Council Directive 2000/43/EC implementing the principle of equal treatment between persons irrespective of racial or ethnic origin of June 29, 2000, 2000 O.J. (L180) 22 may serve as one of many examples for this type of legal act that arguably have been working well and would likely have encountered a number of issues if enacted in a different way.

states. As a result, the common disadvantages of directives substantially outweighed the potential advantages in this case.[90]

For these reasons, the GDPR was enacted with the purpose of enforcing the all-new European fundamental right of privacy, replacing former legislation at both European and national level.[91] As a regulation, the GDPR is directly applicable in all member states, without further steps needing to be taken by national legislatures.[92] This is unlike directives.

The main emphasis of the GDPR is its regulatory function. Its main purpose is the objective of most EU regulation: directing streams of commerce.[93] The GDPR puts an end to differences in national legislation that may "constitute an obstacle to the pursuit of economic activities at the level of the Union . . . ."[94]

Of course, regulation of commerce is not the sole purpose of the GDPR. In full, it aims to "contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons."[95] Even more notable than this combination of market-oriented and privacy-oriented approaches is its additional stated purpose that "[t]he processing of personal data should be designed to serve mankind."[96]

To promote both interests, freedom of individuals and markets, the GDPR provides a rather unusual framework. Although its default opt-in rule requires controllers and processors to obtain the data subject's consent to process data,[97] there are numerous exceptions.[98] These exceptions apply if processing is "necessary" for an enumerated purpose. Thus, consent is the only way to avoid a risky balancing test. For certain categories of sensitive data, consent requirements are heightened,[99] but relying on exemptions and

90. The GDPR recitals admit, in refreshing honesty, that the Data Protection Directive "has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity." GDPR Recital (9).

91. GDPR Recitals (9), (10).

92. TFEU art. 288.

93. Originating from the European Coal and Steel Community, later the European Economic Community and the European Atomic Energy Community, most EU regulation still is found on the economic sector. *See, e.g.*, GDPR, Recitals (5), (7), (10).

94. GDPR Recital (9).

95. GDPR Recital (2).

96. GDPR Recital (4).

97. GDPR art. 6(1)(a); *see also* GDPR Recital (40).

98. GDPR art. 6(1)(b)-(f).

99. GDPR art. 9(2)(a).

their respective balancing tests becomes more perilous due to their further narrowed scope.[100] As a result, the GDPR attaches great importance to the data subject's right to privacy but does not entirely neglect economic purposes.

There are good reasons for this policy. The European Union is frequently credited with establishing peace by economic integration.[101] Therefore, serving both mankind and the free market are inextricably intertwined concepts in Europe. It would be a grave misunderstanding of European politics to think that an economic approach diminishes the integrity of privacy as a fundamental right. The opposite is true. It is a fundamental European insight that mankind is served best where the channels of commerce flourish. Whether Europe is correct in this insight or not, it plays a critical role in European legislation. The European Union therefore has been mainly acting as a regulator throughout its data privacy history. In more recent years, by putting more emphasis on the data subject's individual fundamental right to privacy, the European Union now has been assuming a watchdog role that is similar to, and potentially conflicting with, core functions of its member states' governments.[102]

IV. Future law and policy

The understanding of a law or a legal theory should ideally match both its historical foundations and its policy purposes. At least in part, this is the case for international privacy laws. There are clear traces of the U.S. "right to exclude" approach in its present privacy law, as there are traces of a human rights approach in German and European law.

However, this does not necessarily mean that the effects of present law are always desirable, considering the historical values those legal approaches are based on. In the heat of the moment, overarching philosophical and political values are not always the sole basis of lawmaking. Lawmakers can err, and consistency may not always be politically wise. As a result, the law itself occasionally may seem fragmented. This is especially true for the U.S., but even the European and German systems frequently struggle with their own foundations. Therefore, possible approaches to the future handling of data are considerably different. After having analyzed current legislation by

100. GDPR art. 9(2)(b)-(i).

101. *See, e.g.*, Anastasiou, Harry, *The EU as a Peace Building System: Deconstructing Nationalism in an Era of Globalization*, 12/2 INT'L J. OF PEACE STUD., 31 (34) (2007).

102. This is indicated by the fact that the EU member states continue to have own privacy laws with sometimes different standards.

exploring its respective roots, it is now time to assess trends and possible developments.

A. United States: In search of a common framework

Essentially, U.S. privacy law does not exist as one comprehensive statutory scheme. Of course, apart from specific topical federal laws, there are several comprehensive state laws that deal with privacy interests.[103] These laws show common trends, but their political orientation still varies greatly.

Here, the doctrine of preemption can come into play.[104] Federal preemption automatically invalidates state law that conflicts with federal law. Thus, if Congress elects to use its powers in the field of privacy, this will result in preemption of state privacy laws. The function of preemption is to ensure uniformity in legal areas that are constitutionally allocated to the federal government. In some ways, a preempting data privacy law would be comparable to the GDPR and its effects on national data privacy laws of the EU member states.[105]

However, inhibited by its traditional role as an intruder, the U.S. federal government continues to struggle to fully assume its role as a regulator.

The strongest regulatory approach so far was not initiated by Congress, but by the recent activity of the Federal Trade Commission (FTC). The FTC has powers to regulate business conduct and to prevent "unfair methods of competition in . . . commerce."[106] Because there is no comprehensive federal privacy law, this general rule is frequently applied to the field of data privacy violations.[107] In some respects, the FTC acts as a data privacy agency without being one, and with some success.[108] It is, however, difficult to imagine this to be a permanent solution. Government agencies do not usually benefit from an overly broad scope of duties.

---

103. Namely, the California Consumer Privacy Act [CCPA], the California Privacy Rights Act [CPRA],

the Colorado Privacy Act, the Virginia Consumer Data Protection Act, and the Utah Consumer Privacy Act are considered comprehensive data privacy legislation at state level.

104. U.S. CONST. art. VI § 2.

105. As discussed *supra*, the GDPR does not fully preempt national privacy laws, but it does provide numerous standards that govern both European and national law. Likewise, different degrees of preemption are possible under U.S. law.

106. 15 U.S.C. §45(a)(2).

107. FTC, REPORT TO CONGRESS ON PRIVACY AND SECURITY 1 (2021)

108. *See* Daniel J. Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 590.

The lack of a comprehensive federal framework is why some scholars consider data ownership to be a viable approach in protecting data privacy rights. The U.S. Constitution and Supreme Court precedent strongly emphasize the protection of property rights,[109] while the Court's privacy protections, as shown, suffer from occasional fuzziness. If there is no clear level of protection, why not transfer the well-established protections of property rights to the field of data?

This initially intriguing idea does not withstand stricter scrutiny. It is true that property rights would simplify the protection of privacy interests. However, complexity is an inherent feature of privacy interests that cannot properly be cured by applying incongruous legal concepts to them. To categorize a fundamental right as property means to assign economic value to the right, and to potentially detach it from its holder. Those aspects are core elements of property. If data were subject to some form of modified ownership that did not include key elements of usual ownership rights, there would be no sense in defining data as property. To redefine an existing legal concept both in scope and function means to wipe out its existing form. Instead of doing so, it simply is easier to consider personal data a legal "something," but not property. Ultimately, if there shall be no price tag, there should be no ownership either.[110] Who owns property has both the factual and legal possibility to transfer this ownership. For data, this is not the case.

Thus, the future of U.S. privacy law will not lie in data ownership; nor will it forever remain in the hands of state legislatures. Emphasizing state rights instead of common federal interests does not meet the needs of efficient data protection and privacy, and differing state laws make it more difficult for controllers and processors to comply. This is a no-win situation. Furthermore, the FTC will not be able to bear the burden forever. Public needs, business interests, and international competitive pressures will eventually result in a comprehensive federal data privacy framework that most likely will preempt the already existing fragmented state legislation and have a both unifying and clarifying effect that is similar to the GDPR's. However, this does not say much about the contents of that eventual hypothetical federal law. Undoubtedly, the U.S. will closely monitor legislative developments in Europe.

---

109. *See, e.g.,* U.S. CONST. amend. V. The Due Process Clause explicitly applies to property.

110. *See* Determann, *supra* note 20, at 39-40.

B. European Union: A market for data under the umbrella of fundamental rights

As noted above, privacy is a fundamental right granted by the European Union to the citizens of its member states. Fundamental rights are inalienable. Counterintuitively, the comprehensive GDPR regulation has the main objective of regulating how data is processed.[111] Processing means movement. Thus, the European Union mainly acts to ensure that the stream of data is in constant flux.

When it comes to data streams, the European Union is omnipresent. There is no choice but to comply with its rules, even if private parties might want to agree on different solutions.[112]

In its core values, the GDPR is mandatory and cannot be waived. Compared to the fragmented U.S. privacy law, the mandatory nature of the GDPR is its main strength in protecting consumers. Another strength of the GDPR is to emphasize consent, and not to define it as mere absence of an objection.[113] This opt-in approach ensures that data subjects must explicitly agree to most kinds of data usage.

Because the European Union must appropriately handle a variety of cultural and legal traditions within its borders, the GDPR has chosen a formalist approach instead of narrowly tailored rules.[114] The main goal is to regulate a market, a stream of data, that might not even exist if personal data were indeed an inalienable part of privacy. Only because the GDPR's main objective is to regulate data in transit, not merely data at rest, this stream can continue to exist. Thus, the existence of market regulation itself tends to show that the GDPR does, in fact, embrace business-friendly notions of data privacy. Otherwise, the EU could have chosen to protect data as a truly fundamental right of the individual, and the individual only, without considering any business interests. It admittedly is counterintuitive to call such a comprehensive, formalist regulation "business-friendly." However, regulating a stream of commerce necessarily includes maintaining it.

---

111. GDPR art. 1.

112. The GDPR does not provide waiver mechanisms for its protections.

113. GDPR art. 7.

114. There are few GDPR articles that do not directly or indirectly refer to formal requirements. The principle of accountability, GDPR art. 5(2), might be the most extensive of these duties, effectively incorporating the requirement of being able to prove compliance with all other GDPR principles. However, a formalist approach can also be found, e.g., in the privacy policy requirement, GDPR art. 12(1), the data processing agreement, GDPR art. 28(3), or the mandatory record of processing activities, GDPR art. 30(1).

Each market, to state the obvious, requires not only sellers and buyers but also goods to be sold. The marketability of data, however, affects its legal nature and vice versa. Marketability typically is part of the property "bundle of sticks," i.e., a right that typically belongs to owners of certain assets. But the GDPR does not regulate the legal nature of data. In fact, the GDPR's necessary abstention in the field of property law[115] results in a definition of data that can only be described as circular.[116] That is, the GDPR tells us that data is data without ever attempting to explain what data is in a legal sense.

In conclusion, Europe has already made good use of its legal competences and possibilities. While the opt-in approach alone arguably is not sufficient to emphasize the role of privacy as a fundamental right, the comprehensive and formalist regulation of data streams ensures that data privacy now appears on the agenda of anyone who plans to conduct business in Europe. Future emphasis will be on the enforcement of this legal rule.

C. Germany: Adapting to the GDPR scheme

One might assume that the comprehensive legal scheme of the GDPR does not leave room for national peculiarities. Due to limitations of European lawmaking,[117] this is only partially true.

Despite Germany's human dignity approach, German courts traditionally tended to give private parties more leeway in terms of data usage.[118] Additionally, the formal burdens under German law were less strict

115. Property law is not a competence of the European Union and therefore regulated by its member states.

116. GDPR art. 4(1).

117. TFEU, artt. 3-6, enumerate exclusive and shared competences of the EU. There is an ongoing debate on the position of European law in the hierarchy of national law. The aforementioned "As Long As" jurisdiction, BverfG, Oct. 22, 1986, 73 BverfGE 339, 340, implies that European law only prevails if it is within the limits of domestic constitutional law. This would mean that the constitution remains the "supreme law of the land," as U.S. const. art. VI § 2 puts it, and that it abstractly limits European lawmaking even within the enumerated powers of the EU. In any case, the outer limit for any governmental action on German territory undoubtably is the principle of human dignity, as construed by the Federal Constitutional Court.

118. *See* BGH, May 15, 2018, 218 BGHZ 348. The BGH held that videos of a car accident recorded by so-called dash cams can be admitted into evidence in a civil trial for damages. The court applied a balancing test, weighing the defendant's right to informational self-determination against the plaintiff's interests in using the evidence to prove that the defendant caused the accident. In pre-GDPR times, the balancing test was the applicable standard in determining whether privacy interests were violated. It is of course questionable whether the ultimate result would have been different under the GDPR, but this very late pre-GDPR opinion instructively emphasizes the weaknesses of balancing tests compared to statutory rights.

than under GDPR rules.[119] Thus, even if the GDPR and the German constitutional reality seem closely related at first glance, both the government and private parties still have to adjust.

Again, the result of the assessment seems strange: the former German approach, solely based on human dignity, provided less strict rules than the European approach that is designed to promote and to support channels of commerce. There is an explanation for this apparent imbalance. Human dignity approaches provide strong protection for single individuals but require balancing individual interests against other individual or common interests. In its traditional form, the pure human dignity approach as applied by German courts is ill-suited for regulating conflicting rights on a massive scale. Assuming, arguendo, that most data processing does not violate fundamental rights of a certain individual, the difficult part is to identify acts of violation. There is a common societal interest in any individual's human dignity. But there is no such thing as an individual interest in the dignity of humanity itself. This ultimately amounts to a question of standing, meaning that nobody can act individually on behalf of society in general. This is a clear weakness of pure fundamental rights approaches in the age of "Big Data."

The formalist approach of the GDPR therefore is a potential game changer for German courts. The role of private action traditionally has been limited because German procedural law generally does not allow class actions.[120] This procedural limitation on individuals matches the strong role of the government in enforcing privacy laws. However, providing clear requirements and standards, the GDPR makes individual legal action more attractive.[121] It seems that German lawmakers remain skeptical about legal action by individuals in the field of data privacy: a recent change in German competition law, for example, severely limited possible causes of action for businesses in case their competitors violate formal GDPR requirements.[122]

---

119. Essentially, this resulted from a narrowly scoped definition of personal data that, unlike GDPR art. 4(1), did not include information relating to subjects who are merely identifiable but not identified. By narrowing the scope, regulatory requirements did not apply to many businesses. There is a broad variety of further differences, but for terms of this note it suffices to say that the practical effects of the GDPR have been substantial.

120. This is different in other member states, like the Netherlands. *See* Toby Sterling, *Dutch foundation seeks consumer damages over Apple, Google app payments*, REUTERS (Feb. 16, 2022, 2:36 AM), https://www.reuters.com/technology/dutch-foundation-seeks-consumer-damages-over-apple-google-app-payments-2022-02-15/.

121. It is possible that the EU will provide a class action procedure in the future. As of today, most procedural law is left to the member states.

122. Gesetz gegen den unlauteren Wettbewerb [UWG] [Act against Unfair Competition], translation at https://www.gesetze-im-internet.de/englisch_uwg/. Unfortunately, the translation is not up to date. In its current version, UWG § 13(4) explicitly exempts warnings

Meanwhile, the voices of German data ownership advocates have fallen silent.[123] The legal nature of data apparently does not have any importance for the remaining sovereignty in the field of dignity-oriented privacy. If the debate on ownership rights in data reignites, it would most certainly take place on the European level where the main responsibility for data privacy now resides. Because the area of property law remains in the hands of the member states, however, such a discussion likely would be futile. As a result, one can fairly assume that the GDPR unintentionally has put an end to the already modest German discussion of data ownership. For the reasons stated above, this was a likely outcome from the beginning. Human dignity and ownership rights are strangers to each other.

Therefore, this is not a threshold situation for German law anymore. While human dignity remains the ultimate touchstone for severe privacy violations, the GDPR will continue to handle daily business. As stated above, some room for national privacy law still exists under the GDPR regime, with an emphasis on procedural law. Time will tell how limited the member states' options turn out to be, apart from that. The German approach so far is rather cautious.

V. Sustainable ways to protect public and individual privacy

There are many ways to describe the state of privacy law at the beginning of the second decade of the 21st century. "Uniform" or "consistent" are not terms one can use. However, history and present legislation unequivocally show that there is at least some common ground. A truly sustainable way to protect both public and individual privacy interests requires governments to make use of integral parts of all existing legal frameworks, and to discard other parts of those frameworks. It is a three-step approach, and all are feasible.

First, as the GDPR shows, awareness is key. There is no common notion, in fact there is no notion at all, of data privacy without privacy awareness. To effectively protect privacy interests, both the holders of these rights and their potential violators must be aware of the existence and the scope of such interests. Second, similar to present United States law, privacy

based on GDPR violations from reimbursement claims. Furthermore, UWG § 13a(3) limits possible contractual claims. Without reimbursement, the incentive to issue a warning at own risk is substantially weakened for many businesses.

123. Unlike its predecessor, in setting out political plans of the federal government the 2021 coalition agreement makes no references to data ownership approaches. *See* KOALITIONSVERTRAG ZWISCHEN SPD, BÜNDNIS 90/DIE GRÜNEN UND FDP 17-19 (2021). *Cf.* KOALITIONSVERTRAG ZWISCHEN CDU, CSU UND SPD 102 (2018).

practitioners should advocate for a responsible exercise of individual rights. It is a core principle of all privacy rights that they are open to individual exercise. Third, the German human dignity approach demonstrates that public interests are the outer limit of any individual right. Wherever an individual decision to waive privacy rights, or a decision to ignore such rights, endangers interests of society, a governmental watchdog will be needed.

A. The principle of privacy awareness

Privacy awareness, not to be confused with data awareness,[124] is a core concept in enabling individuals to treat their data responsibly.[125] As such, it is a subtype of media literacy, the ability to critically analyze sources. Privacy awareness describes the skill of understanding the basics of data processing, and making informed decisions based on this understanding.[126]

The terminology in this field can be confusing because it is not properly established. Data science has been focusing on the use of data, not on the rights of the data subject. This resulted in numerous terms that emphasize efficient use of data. Of course, even for privacy purposes it is helpful to know how to properly use data in general. Many privacy violations result from the inability of data controllers to identify data they actually need for their respective purposes. This self-limitation inherent in the term "data awareness" therefore has its own importance, but however important it may be, self-limitation by data controllers is not the key to responsibly exercising privacy rights.

Thus, the term "privacy awareness" more aptly refers to data subjects and their ability to meet controllers at eye level, while "data awareness" rather indicates where eye level will be met. The result of data awareness without sufficient privacy awareness can be witnessed in the present regime: controllers provide the insufficiently informed data subject with information they neither read, nor understand.[127] This obvious disparity is the core of massive criticism of the merely "performative" function certain privacy

124. *See* Moti Gindi, *Data Awareness Is Key to Data Security*, DARK READING (Jan. 20, 2021), https://www.darkreading.com/risk/data-awareness-is-key-to-data-security. This concept may contribute to responsible data usage by businesses but does not help enabling the holders of privacy right to make responsible decisions concerning their data.

125. Stefanie Pötzsch, *Privacy Awareness: A Means to Solve the Privacy Paradox?* (2008), https://link.springer.com/chapter/10.1007/978-3-642-03315-5_17.

126. *Supra* note 120, at 228.

127. *See* Rex Chen et al., *Fighting the Fog: Evaluating the Clarity of Privacy Disclosures in the Age of CCPA* (2021), https://dl.acm.org/doi/pdf/10.1145/3463676.3485601.

practices allegedly have.[128] Formal guidelines and best practice, as provided by most contemporary privacy laws, indeed may lead to data awareness by those who control the data, but it is no appropriate way to raise privacy awareness. Frankly speaking, most people do not care much about privacy policies.

On the other hand, the enactment of the GDPR itself, like the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), did its part to create a certain level of awareness.

First, most data subjects know the controller's perspective to some degree. For employers outside the data industry, it is the legislation – GDPR, CCPA, or CPRA – and the required levels of compliance that constitute their first meaningful contact with the field of data privacy. To be confronted with compliance requirements automatically puts data privacy on the agenda. Many critics focus on the data industry and how privacy legislation affects it.[129] But there is no need to put the issue of data on the agenda of an industry that carries data in its name. On the other hand, even in the age of "Big Data," there are a wide range of industries that are less data-driven, or not data-driven at all. A bakery, for example, may wish to inform its customers via a simple website that works like a newspaper advertisement and is not supposed to have any other function. By requiring this bakery to create a privacy policy for their website, the GDPR may have created privacy awareness. Formal requirements can serve to shed light on problems because such requirements allocate responsibilities for solving them. Asking for compliance means asking citizens to actively address an issue.

Second, the broad scope of this legislation stimulates public debate. While field-specific regulations typically will not generate substantial public interest, comprehensive regulations do. The mere idea of being affected makes this debate a common cause. It is indeed debatable whether, in the grand scheme of things, the average mom-and-pop store should be subject to similar data privacy requirements to the multinational big data behemoth. But the debate that results from the idea of being potentially affected is the main reason general laws are the sharpest sword in the arsenal of governments.

Last, another main idea of recent legislation still might contribute to privacy awareness. The GDPR requires that data subjects be informed "in a concise, transparent, intelligible and easily accessible form, using clear and

128. ARI EZRA WALDMAN, INDUSTRY UNBOUND 30 (2021).

129. *Supra* note 123, at 22.

plain language."[130] Similarly, the CCPA requires businesses to inform consumers about their data-related activities using "plain, straightforward language and avoid[ing] technical or legal jargon."[131]

As pointed out, the current effect of these provisions is debatable at best. To determine whether language is sufficiently straightforward to meet legal requirements is not an easy task. Nevertheless, the existence of such provisions proves that privacy awareness is on the agenda of lawmakers, and in case of the GDPR, violating the provision can trigger its much-admired, or much-dreaded, administrative fine rule.[132] In the medium term, this silent threat might bring forth the intended effects. Otherwise, the European Union could possibly try to enforce this provision, despite difficulties in determining whether a violation occurred. In any case, there is a strong interest in raising privacy awareness by making privacy information more accessible.

Admittedly, to force citizens to confront the vast field of data privacy casts doubt on the honorable notion of privacy as civic self-awareness. On one hand, privacy emerged from individual needs to be left alone. On the other hand, privacy legislation is supposed to make people aware of their own needs. This apparent paradox, the need to actively foster civic self-awareness, bears resemblances to empowerment debates. In fact, structural inequalities are an important feature of the digital privacy imbalance.[133] Similar to empowerment approaches, building awareness is a first step in establishing awareness of one's own conduct, and of rights resulting from that conduct.

B. Responsible exercise of individual rights

Private control is an integral part of privacy rights. Empowerment means assuming responsibility. Because privacy needs differ between individuals, only data subjects themselves can take responsibility here.

---

130. GDPR art. 12(1). This provision itself, referring to five other provisions and including an astonishing number of subordinate clauses, would arguably have benefitted from a greater effort to be concise and easily accessible. Accessibility of data privacy laws is a problem on its own that correlates with general shortcomings in the area of lawmaking and therefore unfortunately cannot be covered here.

131. CAL. CODE REGS. tit. 11, § 999.308(a)(2)a (2020).

132. GDPR art. 83(5)(b), expressly refers to GDPR, art. 12, which establishes the right to clear and concise information.

133. *See* Bhaskar Chakravorti, *Why It's So Hard for Users to Control Their Data*, HARV. BUS. REV. (Jan. 20, 2020), https://hbr.org/2020/01/why-companies-make-it-so-hard-for-users-to-control-their-data.

Exercise of rights requires freedom of choice. True freedom of choice can only exist under an opt-in regime. To rely on opt-out is a central flaw of most privacy legislation. Equally, the clear opt-in regime is a major advantage under the GDPR, albeit diluted by several ways around the checkbox.

Conversely, if there is truly informed and voluntary consent, governmental protections of individual interests are not needed anymore and must be reduced to an appropriate level. To protect individuals who, fully aware of risks and benefits, freely give their consent to use their data would be paternalistic. Privacy rights, by their nature as liberty rights, include the right to self-harm. Therefore, governmental protections may only be provided if consent lacks voluntariness or information, or if other individuals are exposed to unwanted risks.

C. Defending public interest

Most privacy rights, if waived, do not pose direct harm to others.[134] This is different in case of data privacy. By its nature, data always affects others. Each data item that is made available by any individual contributes to a growingly comprehensive network of information that sheds light on formerly opaque areas of privacy.

This public interest requires regulation. There can be no waiver of public interest, and therefore no valid consent to anything that is against public interest. If data processing bears the risk of public harm, public interest must be the touchstone. Mandatory governmental consent in case of especially dangerous activities might be a possible approach, i.e., a "license to process." Data broker registration, as is now mandatory in California,[135] pursues similar goals. It does this by generally assuming that data brokers need additional supervision, and by granting affected individuals additional opportunities to track the usage of their data.

Independent agencies must monitor data streams in general, and sensitive data in specific. Data protection agencies are a necessity.

134. Discussions about indirect, non-individualized harm, e.g., for public morals, will be disregarded for purposes of this note. "Harm" here does refer to violations of legally enforceable individual rights.

135. CAL. CIV. CODE § 1798.99.82(a) (Deering 2020).

VI. Conclusion

The quest of discovering common ground in international privacy law has proven less hopeless than it initially seemed. Existing legislation is ambiguous, and sometimes puts privacy interests in danger instead of protecting them. But the foundations of different privacy approaches are not incompatible with each other. Rather, each approach provides a critical ingredient for a truly modern approach to data privacy that could give guidance and protection without entirely replacing individual liberty with common interest.

There can be no dispute about the importance of data privacy in this day and age. First, Aristotle's idea of privacy became reality at the dawn of Enlightenment, turning this era into an age of privacy. Later, Orwellian totalitarianism endangered privacy interests. Now, and once again, privacy legislation finds itself at a crossroads. Whatever the roots of the various privacy rights, and whatever their historical purposes, all those concepts share common goals.

Future legislation should continue balancing the four essential functions a government can have in the privacy context: the role of intruder, watchdog, regulator, and gatekeeper. Only governments have the power that is required to establish mechanisms of effective protection. Governments furthermore can support their citizen in using their personal data responsibly, but largely at their own discretion. But when acting on the field of data privacy, governments must be aware of their own imminent dangers, of the risk that their different roles may conflict with each other.

Ultimately, the "fuel of our future" has one thing in common with more conventional fuel: however strict the regulation of fuel sales and usage may be, the choice of destination will always be up to the vehicle's driver. It is within the responsibility of governments to put their citizens in the driver seat, provided they have obtained the knowledge needed for handling the task at hand. If a citizen, properly armed with such knowledge, makes a decision, it is another governmental duty to respect and to protect this decision.

Defining the scope of privacy rights can never be left to governments, but governments need to be trailblazers for privacy. Future legislation will have to pave the way, but in the spirit of the Enlightenment, it will be the individual citizen's decision to take it. To venture into a new age of privacy will require both structural and individual efforts, but data privacy as a truly fundamental, truly personal right remains the best option.