IRDG Institut für das Recht der digitalen Gesellschaft

UNIVERSITY OF PASSAU Faculty of Law

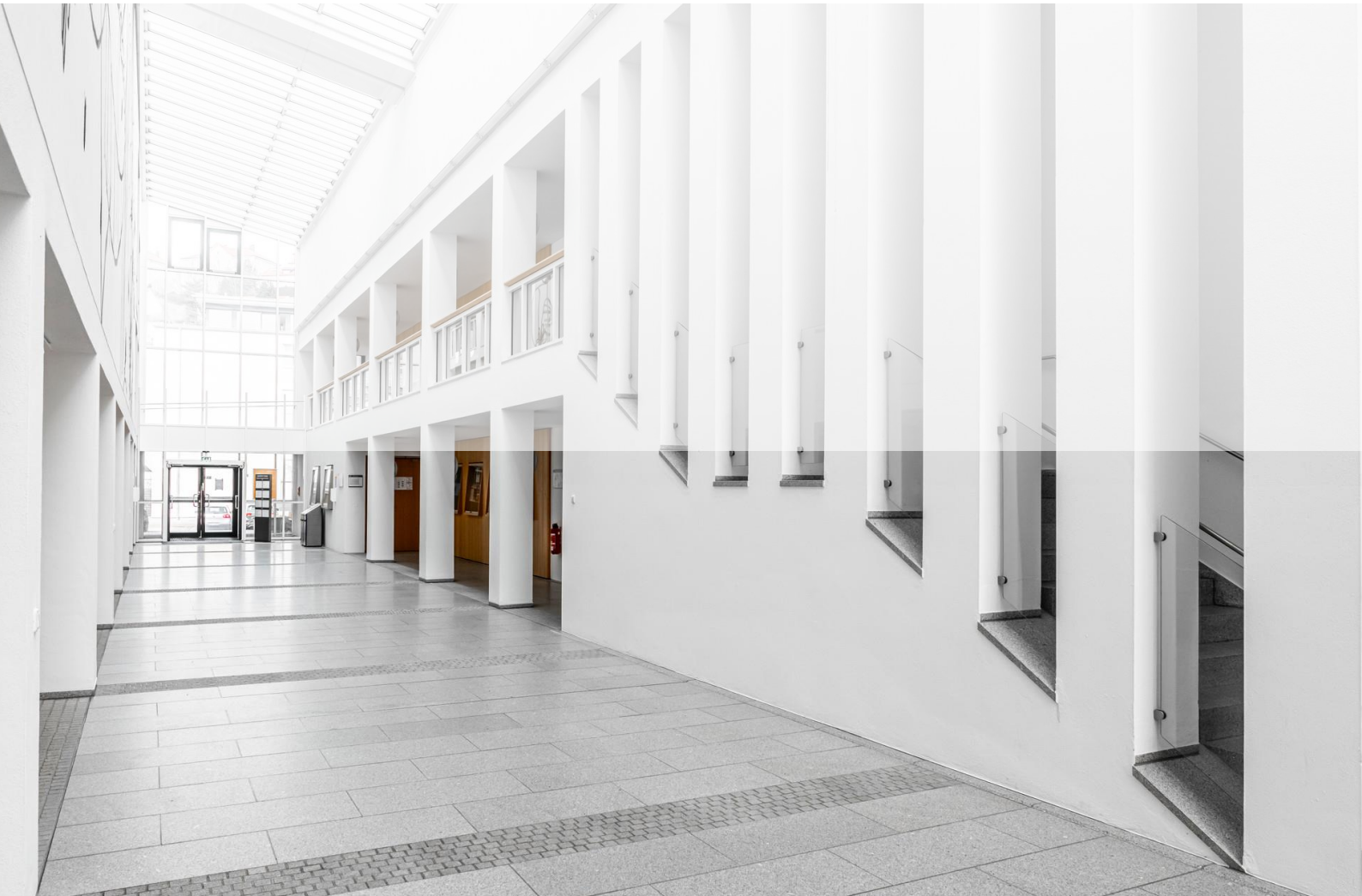
UNIVERSITY OF PASSAU IRDG RESEARCH PAPER SERIES NO. 22-12

LAND OF THE FREE

Legal Country Report on the United States of America*

Benedikt Leven**

December 2021



Place of Publication

University of Passau IRDG
c/o Chair of German and European Private Law, Civil Procedure, and Legal Theory
Innstraße 39
94032 Passau

https://www.jura.uni-passau.de/irdg/

Abstract

About the rough structure of the document: First, addressing the accompanying cultural conditions – which interact with the legal system in the focus – an attempt is made to provide an initial sketch of the 'cultural vectors of data disclosure' in the US (see A.I.1. and A.I.2.). These cultural observations also include initial – general – statements on the legal sphere of data disclosure (see A.I.3. to A.I.6.) and on characteristics of the legal order (A.II.). Subsequently, the information law of the United States is outlined (B.) and finally some details, in addition to the abstract information provided before, of the US data protection law will be given (C.).

Cite as

Leven, B. (2022). Land of the Free - Legal Country Report on the United States of America. *University of Passau Institute for Law of the Digital Society Research Paper Series No. 22-12.* https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/.

Keywords

Digitalisation, United States, Data Disclosure.

Contents

A. Generalities

To set the mood for the analysis of US data protection and information law, some cultural (side)[1] aspects of 'data disclosure'[2] should be brought to attention which influence the legal regulations – although in a legally not clearly subsumable way –, but which can also relate to the individual actor who comes into contact with the regulations outlined later or with the overall defining phenomenon of privacy (for more details, see C.I.1. below).

The attempt will be made not to present an overly one-dimensional picture: Admittedly, it is not easy for 'non-Americans' and 'only legal scholars' to draw an adequate picture of cultural parameters with limited space, especially without in-depth cultural and social science insights and without falling into stereotypes of once own cultural imprint regarding the United States (the loyal *Billy Joel* listener would probably best sum this problem up with an involuntary association such as 'German State of Mind'...).

A consolation for the critical or simply curious reader of this introductory section may be the prospect that some of the topics only touched on in this paper will be the focus of further publications within the research project.

I. Cultural Vectors of Data Disclosure

(Identification of cultural [pre]conditions for individual data disclosure: cultural parameters that may the decision to disclose one's personal data; cultural practices and expectations regarding data disclosure [eg taboos]; data protection and privacy discourse, particularly articulated calls for reform); narratives and stories concerning data disclosure; synonyms for 'Data Protection' and 'Privacy' in the respective language.[3]

1. Cultural Parameters that Might Influence Disclosure of Own Personal Data

While modern narratives now rarely refer to the 'American Dream' that used to be celebrated at every opportunity, and which was certainly interwoven with the promising 'New World' from its beginnings on, it is still noticeable that there is a continuing private-sector pioneering spirit that persists even in times of growing social inequality and a (slowly but surely) dwindling trust in neoliberal promises of salvation – classically: 'Make America Great Again' (And Again And Again ...).

The constant drive for novelty which brings with it an increased willingness to take risks is if nothing else evident in the recent 'Silicon Valley mentality' – and with a clear link to *data* – which has already been valorised in coaching books for self-optimisation enthusiasts (from all parts of the world).[4] It suggests with its pathos for new innovation possibilities at the

---

* This report is part of an interdisciplinary research project on individual data disclosure: Vectors of Data Disclosure – A comparative study on the disclosure of person-al data from the perspectives of legal, cultural studies, and business information systems research, supported by the Bavarian Research Institute for Digital Transformation (bidt). <https://www.bidt.digital/en/vectors-data-disclosure/>.

** The author wishes to thank the project's research associate Sebastian J Kasper for translating the original German version of the report into English, which is available here. The law student assistants – Niklas Ziegler, Lukas Illek and especially Peer Sonnenberg – contributed significantly to this report's success with their research and thought-provoking contributions.

[1] Reference to cultural country report (Lena Kessel).

[2] In the following (for reasons of at least provisional uniformity within the framework of the overall project), 'data disclosure' refers to the revelation of personal data and information.

[3] These guideline texts are meant to facilitate an overview on the structure and content of all of the research project's country reports.

[4] See only Mario Herger, *Das Silicon-Valley-Mindset: Was wir vom Innovationsweltmeister lernen und mit unseren Stärken verbinden können* (Plassen Verlag 2016); Eric Schmidt, Jonathan Rosenberg and Others, *Trillion Dollar Coach: The Leadership Playbook of Silicon Valley's Bill Campbell* (John Murray 2019).

expense of any 'data conservation'[5] that the 'most powerful valley in the world' encourages rash disclosure and consent rather than prudence and restraint.

This is in line with the published reports of those who were able to gain direct insight into the ranks of the 'key players' behind the large US-based social media platforms: Alongside renowned authors such as *Shoshana Zuboff* who had already published her critical observations from a scientific background elsewhere some employees of influential Silicon Valley networks had their say in the highly regarded Netflix production 'The Social Dilemma' from 2020.[6]

The conclusions that can be drawn from these reports can only lead us to the expectation that the average US Americans will not be able to permanently resist the 'brimming'[7] temptations to disclose more and more data: The data-based mode of operation of the large American networks is mainly used to display targeted advertising based the data collected. Not least because of regular dopamine surges which are automatically administered by the seductive architecture of the corresponding technology[8] the (unspoken) goal of the corresponding platform players is to 'tie' users to their networks for longer and longer periods of time consuming content as actively as possible in order to be able to collect more data and display more advertising (keyword: 'surveillance capitalism').[9]

A fundamental and consistent acceptance of responsibility corresponding to the data power that has arisen in relation to the immanent dangers of data misuse is (still) missing. It was not only the writer *Anna Wiener* who, in her very personal memoirs, hinted at the 'young savages'[10] of the World Wide Web not growing a spine.[11]

Long-time platform 'insider' *Jaron Lanier* who now wants to save the world from what he helped set in motion a few years ago publicly and constantly warns against his too uncritical and ignorant former colleagues and gives strong 'arguments for deleting your social media accounts right now'[12]. The statements of a recently published book – 'Inside Facebook'[13] – underline his fears with new urgency in view of the evidently insufficient internal reactions to the diverse documented problems and scandals.

It remains to be said at this point: The world's most notorious 'comprehensive data collectors'[14] – just to name a few, Amazon, Apple, Facebook, and Google – originate from the US.[15] Their success cannot have left the United States' 'data disclosure culture' untouched.

2. Cultural Practices and Expectations Regarding Data Disclosure

The 'Privacy Paradox' is cited by numerous legal authors to point out that consumers in particular have high expectations of data

[5] Translated from German, 'Datensparsamkeit'.

[6] Instructive Soshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* (PublicAffairs 2019).

[7] Translated from German, 'übersprudelnd'.

[8] cf just Adam Alter, *Irresistible: The Rise of Addictive Technology and the Business of Keeping Us Hooked* (Penguin Books 2017).

[9] On this, see Tim Wu, *The Attention Merchants: The Epic Scramble to get inside our Heads* (Vintage Books 2017).

[10] Translated from German, 'junge Wilde'.

[11] Anna Wiener, *Uncanny Valley: A Memoir* (4th Estate 2020).

[12] Jaron Lanier, *Ten Arguments for Deleting Your Social Media Accounts Right Now* (The Bodley Head 2018).

[13] Sheera Frenkel and Cecilia Kang, *An Ugly Truth: Inside Facebook's battle for domination* (The Bridge Street Press 2021)

[14] Rainer Mühlhoff, 'Big Data Is Watching You' in Anja Brejak and Jan Slaby and Others, *Affekt macht Netz: Auf dem Weg zu einer Sozialtheorie der Digitalen Gesellschaft* (transcript 2019).

[15] Scott Galloway, *The Four: The Hidden DNA of Amazon, Apple, Facebook and Google* (Penguin 2018).

protection, but are themselves unwilling to make the necessary (time) sacrifices in the practical handling of their everyday internet use in order to actually live up to this data protection standard.[16]

3. Data Protection and Privacy in the Academic Discussion

There is currently much discussion about US data protection in the legal debate. This assessment should – with a focus to this country report's following content – suffice:

The articulated need for reform in view of the often incomplete and scattered, sectoral oriented, laws will be picked up (A.I.4. below). Some more recently enacted norms at the state level will also be mentioned below (C.I.4.a)bb) below). Finally, the strengthening of the Federal Trade Commission (FTC) in the area of data protection law enforcement which has been discussed consistently will also come up for consideration when taking a closer look at data pricing law (see C.IV.2.c) below).

The concept of 'privacy'[17] can look back on a long and even glorious tradition in the United States:[18] The Americans *Samuel D. Warren* and *Louis D. Brandeis* internationally initiated[19] the protection of privacy with a very important essay.[20] In its reception, this article on the 'Right to Privacy' has even been classified as one of the most influential articles in American law.[21] The two lawyers were motivated to work on this topic by the increasingly sensationalist and, at the same time, more powerful press due to technical developments in the field of photography. The creation of the tabloid press 'The Sun', for example, took place at that time. *Warren* and *Brandeis* tried, for the first time, to rush to help the victims who were at the mercy of the 'shameless progress' by developing common law tort claims for violations of privacy (which was still in its infancy) – at least in certain constellations (see C.III.4.a)aa)(1) below).

Privacy legislation in the late 1960s and early 1970s also originated in the U.S. and not in Europe – as is often assumed.[22]

The term 'privacy' as such is not directly mentioned in the Bill of Rights or in the US Constitution (in the narrower sense) (for legal sources see A.II.2. below).[23] Only in a – subsequently added – annex to the US-Constitution (US Constitution 4th Amendment) a sphere of personal-self-determined life is described to which 'privacy' was also assigned by important Supreme Court decisions (see for more detail C.I.3.a)aa) below).

Privacy is generally considered 'difficult to define'.[24] Even the classical

---

[16] See only Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (7th ed., Wolters Kluwer 2020) 817.

[17] Ulrich Amelung, *Der Schutz der Privatheit im Zivilrecht: Schadensersatz und Gewinnabschöpfung bei der Verletzung des Rechts auf Selbstbestimmung über personenbezogene Informationen im deutschen, englischen und US-amerikanischen Recht*, (Mohr Siebeck 2002), 49 et seqq; Alexander Genz, *Datenschutz in Europa und den USA: Eine rechtsvergleichende Untersuchung unter besonderer Berücksichtigung der Safe-Harbor-Lösung* (Deutscher Universitätsverlag 2013) 39 et seqq.

[18] Elaborately Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (3rd ed., Wolters Kluwer 2020) 41 et seqq.

[19] Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 10 et seqq.; Kai von Lewinski, *Die Matrix des Datenschutzes: Besichtigung und Ordnung eines Begriffsfeldes* (Mohr Siebeck 2014) 37.

[20] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4(5) Harvard Law Review, 193.

[21] cf for example Harry Kalven Jr., Privacy in Tort Law – Were Warren and Brandeis Wrong? (1966) 31 (2) Law and Contemporary Problems, 326 (327).

[22] Furthermore, it was the American entrepreneurial spirit that popularised the ideas already realised in the USA in Germany − and thus inspired the Hessian Data Protection Act, cf G Aichholzer and H Burkert*ublic Sector Information in the Digital Age: Between Marketsublic Management and Citizen's Rights* (Elgar 2004).

[23] Alexander Genz (n 17) 39; Paul M Schwartz and Karl-Nikolaus Peifer, Transatlantic Data Privacy Law (2017) 106 (1) Georgetown Law Journal, 115 (132).

[24] William M Beaney, The Right to Privacy and American Law (1966) 31(2) Law and Contemporary Problems, 253 (255).

philosophical/theoretical demarcation from the area of the commonly accessible, the public,[25] generally provides little clarity. *Daniel J. Solove* has indeed compiled some essential characteristics of 'privacy' – also beyond the so central 'right to be let alone' – in an essay.[26] Fortunately, practical lawmaking and application can be content with a rough definition of those situations that are protected by privacy – without necessitating an abstract definition of privacy.[27]

4. Articulated Need for Reform

The sector-specific approach of US data protection has been – especially in the private business sector (see C.I.4.b) below) – repeatedly and sharply criticised, given the continuing gaps in protection (C.I.1. below) and the ever-increasing threats to the security of personal information in the Internet even despite the 'buffering' effect of the Federal Trade Commission (C.IV.2.c) below – also on the proposal to further expand the FTC's responsibility).[28] Accordingly, a need for reform – towards 'more general' and more comprehensive data protection laws – has been formulated by various bodies (for details see C.IV.1.b) below, for another concrete reform proposal see C.I.7 below). While in individual federal states this call seems to have been heard to some extent by increasingly enacting new laws (see C.I.4.a)bb) below) which contain broader coherent regulation especially for in consumer law, however, at the national level an *omnibus* law (on this and the differing *sectoral approach*, see also C.I.6 below) which could create a common basis for data protection law is for various reasons probably not to be expected in the foreseeable future:[29]

First of all, comprehensive codifications do not seem to correspond to the Anglo-Saxon regulatory habits of the US, which are characterised by the 'common law' (see A.II.1.−3.). Furthermore, it is certainly also decisive that in Congress which is a key legislative body (see A.II.4. below) – given the background of the permanent competition between Democrats and Republicans – no necessary majority is currently to be expected for the time being – neither under the narrow leadership of the incumbent President *Joe Biden* nor in the foreseeable future.[30]

5. Narratives and Stories Concerning Data Disclosure

Against the background of popular leisure activities such as cinema and television, narratives and stories related to data disclosure are sufficiently imprinted in the social consciousness in Europe:

Two gems of (consumer) culture in the United States – at least indirectly related to data disclosure – are the *Wachowskis'* films 'V for Vendetta' and 'Matrix'. Similar to the novel '1984' by the Englishman *George Orwell* which in light of its popularity in the United States can certainly be justifiably mentioned here they deal with sufficient references to the consequences of various (involuntary) 'data revelations' with their *topos* of 'totalitarian surveillance state' as the framework of the respective narratives.

As a somewhat lesser-known Hollywood film, 'Three Days of the Condor' with *Robert Redford*

[25] Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 42 et seq.

[26] Daniel J Solove, Conceptualizing Privacy (2002) 90(4) California Law Review, 1087; in summary Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 44.

[27] Hyman Gross, The Concept of Privacy (1967) 42(1) New York University Law Review, 34, 36.

[28] cf only Woodrow Hartzog and Daniel J Solove, 'The Scope and Potential of FTC Data Protection' (2015) 83(6) George Washington Law Review, 2230 (2267 et seq and note 216 with further references).

[29] Woodrow Hartzog and Daniel J Solove 'The Scope and Potential of FTC Data Protection' (n 28) 2271 et seq.

[30] The implementation of some important social projects is made difficult by this rough division of the political camps in the USA, as former President Barack Obama recently recalled in the memoirs of his political career: Barack Obama, *A Promised Land* (Crown 2020).

in the leading role approaches the topic with a different focus. It concentrates on the work of the secret service which is also related to data and its (thwarted) secrecy. Also mentionable is the film 'Enemy of the State' with a comparable crime thriller character.

Political narratives around the disclosure of data as discussed here revolve around, for example, *Joseph McCarthy* who became famous through his campaign against an alleged subversion of the United States' government apparatus by communists. In addition, *Edward Snowden* and his politically highly explosive disclosure of information as a whistle-blower have been reported on repeatedly in various contexts in recent years.

Finally, the consequences of 'Big Data' are increasingly being discussed: In a way, it is to be expected that the biggest story around data disclosure and its (societal) consequences is just being written – and that we all participate in it (beyond a purely passive spectator status). The international 'internet and data collecting' corporations already mentioned above (A.I.1. above) which even the US individual states still do not face with true determination are (as the true 'crowning glory' of capitalism's creation)[31] becoming more and more powerful and successful – this has even more intensified in times of the ongoing Corona (variant) pandemic –; they know more and more about people all over the world.[32] Without wanting to seriously allude to earlier (science) fiction stories about the 'Brave New World'[33] (*Aldous Huxley*) we can only hope that this development will lead to a data protection-related 'happy ending'.

6. Specific in Language

America's concept of privacy, and with it the definition of 'privacy', has had a formative influence on the whole world against the background of the above-mentioned (A.I.3.) – internationally groundbreaking – article (*Warren/Brandeis*).

With regard to its linguistic use, it should also be noted that the term 'privacy' is not limited to data protection in the US legal sphere.[34] However, this is not an exclusive peculiarity, at least in respect of the German understanding of privacy, which, similar to the US Constitution 4th Amendment (on the sources of law in general see A.II.2. below, on this specific amendment in more detail see C.I.3.a)aa) below) also includes the living space as a private place of retreat.

II. Legal System and Lawmaking

(central characteristics; sources of law and legal hierarchies; classification of legal systems); lawmakers and influential political and societal movements.

The next sections (1.-4.) focus on the United States' legal system in general in order to be able to better classify the sub-areas of information law (B. below) and privacy protection or data protection (C. below) which will be considered in more detail below.

1. Central Characteristics

The brief reception of three important schools of thought from the more recent development of law in the US, all of which emerged in the course of the last century – and thus probably also had a formative influence on the development of the emerging areas of law to which information and data protection law undoubtedly belonged –, seems to be particularly helpful for understanding the legal

[31] Translated from German, 'Krönung der Kapitalismus-Schöpfung'.

[32] cf only Michael Seemann, *Die Macht der Plattformen: Politik in Zeiten der Internetgiganten* (Ch. Links Verlag 2021).

[33] Other authors alike Clive S Lewis, *That Hideous Strength* (The Bodley Head 1945) and *The Abolition of Man* (Oxford University Press 1943) – or Herbert G Wells *The Sleeper Awakes* (Harper and Brothers 1899) – have outlined similar dystopian visions of the future, which do not go without covering data.

[34] Alexander Genz (n 17) 10, 39, 41.

norms surrounding information and data examined in more detail below. It is all the more important to bear these impulses in mind when looking from the perspective of European data protection which is shaped by German law – and thus methodologically quite 'strict' – to the foreign mode of dealing with comparable factual problems of the individuals' 'informational self-determination' in the United States.

According to both 'Legal Realism' (*Oliver Wendell Holmes Jr*) as well as according to 'Sociological Jurisprudence' (*Roscoe Pound*), – two strands of thought[35] that differ in their concrete justifications and intended effects but whose actual consequences for the further development of the legal system can certainly be mentioned in the same breath –, the (judicial) application and further development of the law should not be so much about the definition of abstract terms in order to (later) be able to subsume by means of exact logic a quasi 'predetermined' solution for every problem of the reality of life but it rather is about a consequence-oriented response to the needs of the participants in the particular constellation.

'Law and economics' places jurisprudence somewhat further into the vague service of concretely colliding interests: It gives a generous free pass away from abstract ideas of justice – which, after all, can also be incorporated much more consistently and comprehensibly in the classical normative constructs criticised by *Pound* as 'mechanical'[36], which are inspired by a larger conception of order and (therefore) have to be methodically stringently coordinated in between each other – by placing the striving for 'macroeconomically' meaningful results in the foreground. The intended 'overall societal'[37] increase in prosperity was never denied here.

These approaches correspond, perhaps not entirely coincidentally, with the practical needs of an international 'superpower' which presumably did not want to endanger its position of power secured after the world wars – through the influence of the US dollar on the currencies of other nations, cemented in Bretton Woods, and thus inevitably also on the global economy – by too 'narrow-minded' legal principles and subsumptions but rather wanted to promote the freedom of the economy for the purpose of the greatest possible utilisation of the acquired prime status in the world economy at any price.

As a result, the conceptual protection of privacy suffered greatly because the practical and loose concentration on the economy as a whole in dealing with concrete danger situations for privacy concerns (see only the 'Data Industrial Complex' proposition[38]) did not lead to a 'bottom-up' thriving and thus finally culminating in a grand structure of a comprehensive overall guarantee but rather to a confusing patchwork of often short-sightedly and too narrowly defined regulations in order to allow the free market economy to flourish undisturbed even in very similar situations.

In any case, the criticism of the inconsistent data protection in the US expressed in numerous academic publications (on this already A.I.4. above and C.I.1. below) should be taken even more to heart against this background.

2. Legal Sources and Their Hierarchy

In the federation of the United States, sources of law are on the one hand at the level of the federal government ('federal law') and on the

[35] Instructive Mathias Reimann und Hans-Peter Ackmann, *Einführung in das US-amerikanische Privatrecht* (2nd ed. C.H. Beck 2004), 8 et seqq.

[36] Roscoe Pound, 'Mechanical Jurisprudence' (1908) 8(8) Columbia Law Review, 605.

[37] Translated from German, 'gesamtgesellschaftlich'.

[38] See Shawn M Powers and Michael Jablonski, *The Real Cyberwar: The Political Economy of Internet Freedom*, (University of Illinois Press 2015).

other hand at the level of the individual states ('state law'): In principle, the federal government and the individual states are on an equal footing; only in areas in which the federal government has explicit legislative competence does it regulate substantive issues in a binding manner for the individual states.[39] If it does so, federal law takes primacy over the law of the individual states in accordance with the so-called 'Supremacy Clause'.[40]

Federal law consists first of all of course of the Constitution of the United States ('US Constitution'), of the 'basic' federal statutes ('Federal Statutory Law'), and the state treaties concluded by the Federation.[41]

Regarding the Federal Constitution, it is worth mentioning that it has received some very significant 'annexes' or 'amendments' in which (modern democratic) central guarantees have been included while the basic text has hardly changed.

The states have their own constitutions and retain in all sectors of competence not transferred to the federal government by the federal constitution the right to enact state law, US Constitution, Art I(8) and US Constitution Amendment X.[42]

Finally, case law is also important – both at the federal level and at the level of the individual states: The US legal system of the 'New World' has its historical roots in English law (of the immigrants) and was initially characterised purely by common judge-made law, ie case law.[43] Since about the end of the 19th century, however, the importance of 'written law' has steadily increased, so that today we speak of a 'mixed' system – with a continuing emphasis on case law aspects.[44] Thus, the judicial practice of the highest courts – which is binding for any interpretation[45] – serves to interpret the content of certain (abstract-general) legal norms.[46] Important court decisions are therefore frequently mentioned below to provide detailed understanding of the information or data protection legal system and to put them in context to the corresponding regulations.

3. Belonging to Legal Systems

As a 'settled colony', which at the time before the English occupation did not yet have a functioning legal system in the modern sense[47], the parent legal system of US American law became – as already mentioned in relation to the case law (A.II.2. above) – English law which has remained very influential to this day.[48]

Nevertheless, classifying American law as part of the 'common law' seems too sweeping; it does not do justice to the diversity of the individual states. For other traditions have also exerted an influence: Louisiana, for example, has followed the French legal tradition – and other states have also been influenced by the Spanish-French approach.[49]

It is therefore appropriate to speak of a genuine, 'Anglo-American' legal system[50] which in its diversity offers room for all the special features of the US.

---

[39] Kirk W Junker, 'US-Recht als ausländisches Recht' in Kirk W Junker (ed), *US-Rechtspraxis* (De Gruyter 2018), 18 et seqq.

[40] Peter Hay, *US-Amerikanisches Recht* (7th ed., C. H. Beck 2020) 6.

[41] ibid.

[42] ibid 22.

[43] ibid 1.

[44] ibid 5; Alexander Genz (n 17) 76.

[45] Peter Hay (n 40) 6.

[46] ibid 7.

[47] cf Konrad Zweigert and Hein Kötz, *Einführung in die Rechtsvergleichung auf dem Gebiete des Privatrechts* (Mohr Siebeck 1996) 215 et seqq.

[48] Peter Hay (n 40) 4.

[49] ibid with further references.

[50] With further references Dieter Blumenwitz, *Einführung in das anglo-amerikanische Recht: Rechtsquellenlehre, Methode der Rechtsfindung, Arbeiten mit praktischen Rechtsfällen* (C. H. Beck 2003) 3.

4. Lawmakers and Influential Political and Social Movements

On the federal level the US-Congress is responsible for law-making which is further divided into the Senate and the House of Representatives, US Constitution, Art I § 1.[51] These two bodies act jointly and equally as legislators. The President has a comprehensive veto right in the legislative process.

At the state level, as far as can be seen, only the parliament, which normally also consists of two chambers[52], is referred to as the legislative body.

From a German perspective, the influence of the courts – out of sheer habit to the political heavyweight 'Federal Constitutional Court'[53] – should not be overestimated: In America, the principle of judicial restraint is much more distinctive than in Germany. Of all constitutional bodies, judges have the least democratic legitimacy and should therefore 'respect', as far as possible, other bodies' decisions, particularly those of the legislature.[54]

However, politics in the United States are influenced to a large extent by interest groups and associations. There are thousands of such associations in the US which in their activities can invoke their constitutionally guaranteed right to petition the government for redress of grievances, cf the US Constitution 1st Amendment.[55]

B. Legal System of Information Law

For the factually and substantively broad general US 'information law system' – on the data protection law system (in the broader sense) see only C below – it is characteristic, even if the headings of this report in the following sometimes suggest otherwise, that there are no overarching norms which uniformly and structurally shape the entire information law system (on its background, see already A.II.1. above). Rather, only area-specific regulations can be found leaving open gaps in protection or (so far) non-guaranteed phenomena.

I. Structure of Information Law

(constitutional and basic rights aspects; relevant regulations concerning intellectual property, secrecy, cybercrime [data privacy *aut idem infra* at C.]; Which regulations are based on international provisions [especially concerning intellectual property]?)

1. Constitutional and Basic Rights Aspects Concerning Intellectual Property

Even if the US Constitution 1st Amendment's spill-over effect on the information law, which will be examined in more detail below (C.I.3.a)bb) below), should not be underestimated, US Constitution, Art I § 8(8), is the direct constitutional basis for patent and copyright law.[56] Central to its interpretation is the decision *Wheaton v. Peters*, 33 US 591 (1834) – the first decision of the United States Supreme Court on copyright.

For patent law, the United States Code (U.S.C.), Title 35, should be noted as an

[51] With in-depth notes on the composition of the individual legislative bodies (and on the rough course of the legislative procedure), see Peter Hay (n 40) 18 et seqq.

[52] ibid 29.

[53] cf only Michael Stolleis, *Herzkammern der Republik: die Deutschen und das Bundesverfassungsgericht* (C. H. Beck 2011); insofar critical Matthias Jestaedt, Oliver Lepsius and Others, *Das entgrenzte Gericht: Eine kritische Bilanz nach sechzig Jahren Bundesverfassungsgericht* (3rd ed., Suhrkamp Verlag AG 2019).

[54] Birgit Oldopp, *Das politische System der USA: Eine Einführung* (2nd ed., Springer 2014) 104.

[55] Instructive ibid 135 et seqq with further references.

[56] US Constitution, Art. I(8), <https://constitution.congress.gov/browse/article-1/section-8/#:~:text=The%20Congress%20shall%20have%20Power,uniform%20throughout%20the%20United%20States%3B&text=1%20Taxing%20Power,ArtI> (last accessed on 18 November 2021).

'important statutory basis' – and for copyright law Title 17, §§ 101 et seqq, 201 et seqq, 301 et seqq. These provisions define the conditions, duration, and limitations of protection. Trademark law is essentially derived from the Lanham Act (15 U.S.C. §§ 1051 et seqq).

2. Access to Information

The Privacy Act not only contains data protection provisions for public bodies at the federal level as part of the data disclosure legislation (see C.I.4.a)aa)(1) below). It also ensures that individuals can access personal information about them held in 'Systems of Records' at federal agencies – which eventually amounts to a right to information.[57] The Freedom of Information Act, passed in the same year (and also at the federal level), provides, subject to the exceptions laid down – and thus in line with the later passed German Freedom of Information Act (GerFoIA) –, for more general access to information from federal authorities[58].

At the state level, each state has its own access to information law which is usually based on the federal law (mentioned above).[59]

3. Cybercrime and Cybersecurity

In the sector of cybercrime and security various regulatory *topoi* have to be distinguished:[60]

'Cybercrime' regulations that inflict penalties for highly technical offences are in particular:

- The 'Federal Computer Fraud and Abuse Act' (CFAA), 18 U.S.C. § 1030, is the most important law to punish cybercrimes – such as hacking attacks – and allows for civil and criminal penalties.
- The 'Economic Espionage Act', 18 U.S.C. §§ 1831-1839 defines 'Criminal Acts' in particular to protect trade secrets.

The 'cybersecurity' sector – ie the (more) preventive design of the security of the internet – is shaped in particular by the following laws:

- On the basis of the 'Cybersecurity Act'[61] of 2015, private economic actors are obliged to exchange information on reportable (cyber-attack) incidents with each other and with the relevant public authorities. 'Title I' of the Cybersecurity Act, also referred to as the 'Cybersecurity Information Sharing Act' (CISA), aims at the productive sharing of information particularly between companies in the implementation of the Gramm-Leach-Billey Act, the Health Insurance Portability and Accountability Act, and some state laws (such as N.Y. Penal Law §§ 156.05, 156.20 et seqq).
- The 'Cybersecurity Enhancement Act' (2014) requires the National Institute of Standards and Technology (NIST) to further develop industry-specific

[57] cf only Privacy Act 1874, <https://www.justice.gov/opcl/privacy-act-1974> (last accessed on 18 November 2021).

[58] Alexander Genz (n 17) 52 et seq.; Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 630 et seqq; see also Freedom of Information Act, <https://www.foia.gov/about.html> (last accessed on 18 November 2021).; On the (constitutional) legal derivation of the right of access to public documents: Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 648 et seqq.

[59] Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 632.

[60] For a detailed overview, see Cybersecurity 2021, ICGL, <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa> (last accessed on 18 November 2021). For further surveillance regulations to guarantee national security - also abroad - see for example Daniel J Solove and Paul M Schwartz, *Privacy, Law Enforcement, and National Security* (3rd ed. Wolters Kluwer 2020), 171 et seqq.

[61] Instructive Sullivan and Cromwell LLP, *The Cybersecurity Act of 2015* (2015), <https://www.sullcrom.com/siteFiles/Publications/SC_Publication_The_Cybersecurity_Act_of_2015.pdf> (last accessed 18 November 2021). Attention: There are also legal acts with exactly the same title ('Cybersecurity Act') at the European level and in other parts of the world.

guidelines and best practices for private companies to defend themselves against cyber-attacks.

- The 'Federal Cybersecurity Enhancement Act' (2016), like the Federal Information System Modernisation Act (2014), directs the United States Department of Homeland Security (DHS) to provide critical cybersecurity services and infrastructure so that federal agencies can easily implement contingency plans.
- On the basis of the 'Cybersecurity and Infrastructure Security Agency Act' (2018) a new agency – the Cybersecurity and Infrastructure Security Agency (CISA) – within the Department of Homeland Security has also been established to protect 'critical infrastructure' in the field of cybersecurity.

Furthermore, two legal acts are significant for the security of the network[62] (in a broader sense):

- The 'Electronic Communications Protection Act' (ECPA), 18 U.S.C. § 2702, is designed to protect electronic communications.
- The 'K-12 Cybersecurity Act' was enacted in October 2021 to protect the particularly sensitive information that is bundled in schools.

Since the influential 'World Economic Forum' never tires of pointing out the unimagined dangers of a 'cyber-attack' in the modern globalised interconnected world and – for example with simulations such as the 'Cyber Polygon'[63] – provides for broad research and discussion material, further regulations in the area outlined here will probably follow shortly (also and especially in the US).

4. Surveillance (in a broader sense)

Another important sector in the area of information law are regulations relating to (especially digital)[64] investigation and surveillance measures.[65]

- The Federal Electronic Surveillance Law – 'Title III' – is regulated in 18 U.S.C. §§ 2510 et seqq:
  - The '*basic* law', if you will, in this section is the 'Wiretap Act', 18 U.S.C. §§ 2510-2522.[66]
  - For the transmission of communications as such, the 'Federal Electronic Communications Privacy Act' (1986)[67] is relevant.
  - The 'Stored Communications Act' (SCA), 18 U.S.C. §§ 2701-2711[68], contains specific regulations for previously recorded and stored communications.
  - The 'Pen Register Act', 18 U.S.C. §§ 3121-3127,[69] regulates records of dialled telephone numbers (and modern equivalents) not covered by other laws concerning communications.
  - The 'Communication Assistance for Law Enforcement Act' (CALEA), also called the 'Digital Telephony Act', aims – beyond the basic Federal Electronic Surveillance – that surveillance technology can already be built into the a devices' 'hardware' to enable later interception by authorities.[70]
- Since 1978, the 'Foreign Intelligence Surveillance Act' (FISA) has granted special possibilities for action in the case of threats to national security or suspected terrorism. For example, 'National Security Letters' (NSL) can be issued to compel telecommunication providers, banks, and

[62] Translated from German, 'Netzkonstrukt'.

[63] Cyber Polygon, <https://cyberpolygon.com/> (last accessed on 18 November 2021).

[64] On 'Search and Seizure' provisions authorising 'physical-spatial' searches to scan, for example, computers or other electronic devices that (might) contain email and online communications, internet service provider accounts, IP addresses, internet search queries, etc.: Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 123 et seq.

[65] On further regulation concerning surveillance addressed to the state: ibid 120 et seqq.

[66] ibid 109, 111 seqq.

[67] ibid.

[68] ibid 114 seqq.

[69] ibid 116.

[70] ibid 117 et seq.

financial companies to disclose data. In relation to foreign countries, the FISA also authorises counter-intelligence.

- In 2001, primarily in response to the attacks on the World Trade Center, the 'USA PATRIOT Act' ('Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act'), 18 U.S.C. § 2331,[71] was enacted to facilitate the investigation of federal authorities in the event of a terrorist threat.
- The 'Countering Foreign Propaganda and Disinformation Act' (original – intended – title: 'Countering Information Warfare Act') as part of the 'National Defence Authorisation Act' in 2017 – after the globally discussed US elections – placed the powers to take security measures abroad on an even broader basis, in the service of the attacked democracy, to prepare for actions against disinformation and propaganda.
- For the sake of proportionality, the 'Federal Communications Act' in 47 U.S.C. § 605[72] prohibits unauthorised use of material collected during surveillance.

In the face of the international advance of ideas of digital identity – cf only the discussions about ID2020[73] – solutions to avoid dystopian control in the area of surveillance, measures will certainly have to be found in the USA as well in order to protect the (equal) freedom of citizens that is so central to democracy.[74]

II. Allocation of Informational Legal Positions

(commodity/commoditization, especially 'intellectual property'; collective goods; public goods)

Provisions about the allocation of informational legal positions are specifically found in the law of intellectual property:

1. Copyright

The US 'copyright' system basically follows an approach based on actual conditions when it comes to allocation: while the right initially lies with the author it can pass to the intended user(s) according to the (economic) utilisation (cf 17 U.S.C. § 201(a) and (b)). Registration can be useful to create clear conditions (17 U.S.C. § 408(a)). Thus, the copyright symbol (17 U.S.C. § 401) serves as a special indication of ownership which can also exonerate in legal disputes, see 17 U.S.C. § 401(d) and § 412.

2. Patent Law

For ownership or attribution of the patent, see 35 U.S.C. § 261 – the patent is treated as 'personal property'.

An application must be filed for its registration, 35 U.S.C. §§ 111 et seqq.

3. Trademark

The relevant 'Lanham Act' already mentioned above (B.I.1.) stipulates that a corresponding application must also be made for the use of a trademark (cf 15 U.S.C. § 1051(a)(1)) – and thus presupposes, as it were, that the owner of the trademark is entitled to make this application (without defining this ownership more precisely).

Once registered, this is regarded as *prima facie* evidence of the validity of a trademark, the legal position of the trademark owner, and his exclusive right to use it (15 U.S.C. § 1115(a)).[75]

III. Institutions

(information supervisory authorities; private institutions/organisations [industry and sectoral

[71] ibid 118 et seqq.

[72] ibid 108 et seq.

[73] Digiatal Identity Alliance, ID2020, <https://id2020.org/> (last accessed on 18 November 2021).

[74] Francis Fukuyama, *Identität: Wie der Verlust der Würde unsere Demokratie gefährdet* (Hoffmann und Campe 2019) 66.

[75] On the trademark symbol see also 15 U.S.C. § 1111.

associations], including international ones; public administration und cultivation/management of informational goods)

Central institutions of US intellectual property law are the Copyright Office (17 U.S.C. §§ 701 et seqq) and the United States Patent and Trademark Office, 35 U.S.C. § 1.

It follows from 17 U.S.C. § 506 that the U.S. Department of Justice also takes action in cases of copyright infringement.

In addition to the agencies already mentioned (see B.I.3. above) – 'DHS' and 'CISA' – police forces and intelligence agencies – Criminal Intelligence Agency (CIA), Federal Bureau of Intelligence (FBI), National Security Agency (NSA), the so-called 'Intelligence Community' – are responsible for internet-related security, crime prevention, and surveillance measures.[76]

IV. Procedural Aspects

(control and enforcement; individual; collective; through associations; by authorities [executive and judicial])

For individual legal enforcement (in particular) general legal actions can be taken:

In copyright law, the 'Federal Court' is responsible for disputes between private individuals; the U.S. Department of Justice intervenes in the prosecution of criminally relevant infringements[77] – see already B.III. above. In patent law, the 'Federal Court' is also the competent court for civil actions.[78] For proceedings in trademark law, it should be noted that jurisdiction is divided between the State and Federal Courts.[79]

Collective agents and collective enforcement mechanisms, comparable to the European or German *Abmahnverein*[80] and consumer protection associations, do not exist:

The entities with standing to sue in a given sector are clearly and conclusively defined in the areas of copyright (17 U.S.C. § 501), trademark (15 U.S.C. § 1071), and patent law (35 U.S.C. § 281).

In addition to these directly authorised parties, third parties (including interest groups) who wish to participate in ongoing proceedings can only participate as 'companions'[81] as 'Amicus Curiae' in civil litigation – by way of a statement, if and to the extent that they can demonstrate a sufficiently plausibly demonstrated interest in the matter.

In addition, a class action remains possible if the infringement is also an unfair or deceptive act within the meaning of the 'Federal Trade Commission Act' (FTCA).[82] However, as will be explained below – for class action see C.III.4.b) et seq. below) – each party must be entitled to bring an action and must be able to demonstrate an infringed interest.

---

[76] Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 438.

[77] US Copyright Office, FAQ, <https://www.copyright.gov/help/faq/faq-infringement.html> (last accessed on 18 November 2021).

[78] Louis E Fogel and Shaun M Van Horn, 'At a Glance: patent enforcement proceedings in USA' (Lexology) <https://www.lexology.com/library/detail.aspx?g=50d0f744-f3f5-4428-bc37-5dbc591c00cf> (last accessed on 18 November 2021); Justia, Enforcement on Patent Rights, <https://www.justia.com/intellectual-property/patents/enforcement/> (last accessed on 18.11.2021).

[79] ICGL, <https://iclg.com/practice-areas/trademarks-laws-and-regulations/usa> (last accessed on 18 November 2021).

[80] These are associations whose purpose it is to fight anti-competitive practices.

[81] Translated from German, 'Mitstreiter'.

[82] cf Martin Schmidt-Kessel, Claas Christian Germelmann and Others, *Die Regulierung des Datenschutzes und des Urheberrechts in der digitalen Welt: Eine vergleichende Untersuchung zu den USA, Großbritannien, Frankreich und Schweden* (Jenaer Wissenschaftliche Verlagsgesellschaft 2015) 58; for trademark law see also Dennis S Corgill, 'Die Bekämpfung unlauteren Wettbewerbs in den USA' (2012) 12 *GRUR* 1065.

C. Regulations Concerning Disclosure of Personal Data

I. Legal Structure of Data Disclosure

(existence of 'Data Protection Law'; mandatory and nonmandatory regulation; differentiation between public and private sector; public or private sector as a role model for regulation; general or sectoral regulation; self-regulation [codes of conduct]; basic principles of regulation [preventive ban or freedom of processing]; risk-based approach [potential for misuse; protection of certain categories of data]; privileged areas [personal and family sphere; media; research])

1. Existence of 'Data Protection Law'

Even if the general rule of law[83] and the central role of the individual – through general binding to a catalogue of fundamental rights ('Bill of Rights')[84] – represent quite fundamental commonalities of European and American data protection law, these parallels between the two legal concepts of protection (which are logically based on the individual's private sphere) cannot, however, hide the fact that the understanding of data protection in the United States is quite different from the one we are familiar with in Europe and thus also in Germany (which is now strongly influenced by European regulations):[85]

First of all, the 'connecting factor' of protection in the US is different from that in Europe: while the General Data Protection Regulation focusses on 'data' as such and builds a comprehensive concept of guarantees around it, in the United States privacy in itself is considered an interest worthy of protection – without 'data' being even broadly and uniformly defined (see C.II. below). In this respect, US privacy protection, which will now be described in more detail, is in a way only the functional equivalent of a 'real' *data* protection right.

Against the background of the above-mentioned general schools of thought, which often ensured the greatest possible market freedom in the development of law in the economic area of the USA (A.II.1. above), this has led to the fact that data protection law has not been able to evolve into a self-contained system with many uniform guidelines – which only seems logical if no general basis has been found even for the so fundamental definition of 'data'.

The consequence of this is that a comprehensive standard of data protection cannot be guaranteed[86] because where simple legal regulations are lacking only the less specific right to privacy provides the basis for the protection of personal data.[87] The many scattered laws literally provoke gaps in protection (those are always only becoming apparent *ex post*).[88]

2. Legal Sources Regarding Data Protection: Overview

Data protection law in the USA, which shapes privacy (see C.I.1. above), has become a – more or less interwoven but by no means transparent – web of different components:[89] These are roughly

- constitutional law and

[83] Peter Hay (n 40) 16.

[84] ibid 32.

[85] cf only Manfred Weber, 'Europäische Standards für den weltweiten Datenschutz' (2009) 2 Zeitschrift für Außen- und Sicherheitspolitik 182, 188. With a more detailed comparative analysis of the individual instruments of the regulatory regimes of European and US data protection: Paul M Schwartz and Karl-Nikolaus Peifer (n 23) 115 et seqq.

[86] cf Hans J Kleinsteuber, 'Rundfunkaufsicht zwischen Regulierung und Governance' in Patrick Donges (eds), *Von der Medienpolitik zur Media Governance?* (Halem 2007) 49.

[87] Alexander Genz (n 17) 42.

[88] Positively verbalised, however, this also never burdens the data recipients without a concrete reason.

[89] Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 2; Charlotte A Tschider, 'Experimenting with Privacy: Driving Efficiency Through a State-Informed Federal Data Breach Notification and Data Protection Law' (2015) 18 Tulane Journal of Technology and Intellectual Property 46, 52.

- 'simple' statutory law – both at the level of the federal state as a whole and at the level of the individual states (on sources of law, see A.II.2. above).

The relevant statutory law consists of

- Some (to a certain extent) general data protection provisions,
- plenty of specific data protection provisions,
- tort and criminal law,
- contract law,
- occasional rights to refuse to give evidence, and
- (according to some authors also) property law.

In the following, after a look at the constitutional law (3.), the focus will be on the general, 'simple' statutory law (4.). With regard to the latter, a distinction is made between federal and state law which addresses either state agencies (the 'public sector') or private (economic) actors (the 'private sector') when they come into contact with certain privacy issues.

In parallel to statutory law, some judicial decisions, in particular those of the Supreme Court of the United States, will sometimes also be discussed – on the background, see A.II.2 above.

As has already been noted in related essays:[90] The US data protection law's differentiated scope requires some kind of focus; unfortunately, 'completeness' cannot be achieved (also and especially) in this working paper.

For further and more in-depth research, the 'Restatements of the Law' of the 'American Law Institute', which lend a certain structure to the broad pool of US legal sources, could provide helpful assistance.[91] Although these 'Restatements' are not legally binding, they systematically present the common law in particular and can thus help to provide a quick overview.[92]

In addition, the use of the following databases is recommended:

- 'LEXIS' and 'Westlaw' are good search engines, especially for court decisions,
- 'HeinOnline' covers numerous periodical publications.[93]

3. Constitutional Law

The US constitutional law exclusively addresses public agencies or, rather, the public sector of data recipients.

a) Federal Constitutional Law[94]

At the federal level, it should first be noted with regard to constitutional law that the original text of the Federal Constitution – which, historically speaking, is quite old for this context[95] – does not provide for direct protection of privacy (let alone protection of personal data).[96]

aa) US Constitution 4th Amendment

The wording[97] of the US Constitution 4th Amendment[98], which is quite abstract, contains a vague reference to the security of

[90] In this regard, Alexander Genz (n 17) 43.

[91] Instuctive ibid 78 et seqq.

[92] Peter Hay (n 40) 12.

[93] ibid 13 et seq.

[94] For more information see Philipp Wittmann, *Der Schutz der Privatsphäre vor staatlichen Überwachungsmaßnahmen durch die US-amerikanische Bundesverfassung* (Nomos 2014).

[95] cf only Peter Hay (n 40) 17 with further references.

[96] Paul M Schwartz and Karl-Nikolaus Peifer (n 23) 115, 132; Manfred Weber (n 85) 182, 188.

[97] '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'.

[98] Instructive on the US Constitution 4th Amendment, Alexander Genz (n 17) 44 et seqq; Paul M Schwartz and Karl-Nikolaus Peifer (n 23) 4 et seq; William J Stuntz, 'The Distribution of Fourth Amendment Privacy' (1999) 67(5-6) George Washington Law Review 1265.

personal privacy. Only on the basis of numerous decisions, however, did its significance for data protection become clearer. Individual privacy has, thus, received – at least in some areas – significant protection from state intervention.[99]

Probably the best known Supreme Court decision is *Olmstead v United States*, 277 US 438 (1928)[100] which addressed the question of whether a right to privacy, which is immanent to the US Constitution 4th Amendment, protects against the use as evidence of recordings of private telephone conversations obtained without a warrant. Another frequently cited decision, *Katz v. United States*, 389 US 347 (1967)[101], established the so-called 'Katz test' to determine whether there is a reasonable expectation of privacy protection in a particular case.

Other significant[102] decisions concerned

- contraception in marriage ('marital privacy'), *Griswold v Connecticut*, 381 US 479 (1965)[103],
- the use of electronic monitoring devices, *United States v Knotts*, 460 US 276/281 (1983),
- abortion, *Roe v Wade*, 410 US 113 (1973),[104]
- the protection of data originally circulated voluntarily from subsequent disclosure by third parties ('Third Party Doctrine'), *Smith v Maryland*, 442 US 735 (1979)[105],
- GPS tracking of a vehicle, *United States v Jones*, 565 US 400 (2012)[106],
- the possibility of utilising the detection of a (prohibited) stock of marijuana made outside of a restricted area, *Oliver v United States*, 466 US 170 (1984).

In summary, the State and its organs may only take note of private matters if there is an adequate reason to do so. However, comprehensive privacy protection is not guaranteed by the US Constitution 4th Amendment, even as interpreted by the Supreme Court.[107]

Rights under the constitutional amendment can follow from the so-called 'Exclusionary Rule', which is tantamount to an exclusion of illegally obtained evidence – or can be enforced through civil claims.[108]

bb) US Constitution 1st Amendment

Some courts and scholars see at least rudimentary points of contact between the 'right to privacy' and the US Constitution 1st Amendment which protects freedom of

---

[99] Alexander Genz (n 17) 47; Manuel Klar and Jürgen Kühling, 'Privatheit und Datenschutz in der EU und den USA - Kollision zweier Welten?' (2016) 141(2) Archiv des Öffentlichen Rechts, 165, 39.

[100] Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 35; Daniel J Solove and Paul M Schwartz, *Privacy, Law Enforcement, and National Security* (n 60) 12 et seqq.

[101] Daniel J Solove and Paul M Schwartz, *Privacy, Law Enforcement, and National Security* (n 60) 22 et seqq.

[102] Two additional - somewhat less cited, but arguably still worth noting – US Constitution 4th Amendment-related rulings are *Cardwell v Lewis* 417 US 583 (1974) and *Lopez v United States* 373 US 427 (1963) – on this: Daniel J Solove and Paul M Schwartz, *Privacy, Law Enforcement, and National Security* (n 60) 20 et seqq.

[103] Daniel J Solove and Paul M Schwartz *Information Privacy Law* (n 16) 565 et seqq.

[104] The constitutional assessments introduced by *Roe v Wade* could soon be open to at least a partial reassessment by a still pending decision in front of the US Supreme Court, see only *Liptak, Adam*, Supreme Court to Hear Abortion Case Challenging Roe v. Wade, The New York Times, 17 May 2021 (updated 1 December 2021), <https://www.nytimes.com/2021/05/17/us/politics/supreme-court-roe-wade.html>.

[105] Daniel J Solove and Paul M Schwartz, *Privacy, Law Enforcement, and National Security* (n 60) 33.

[106] ibid 70 et seqq.

[107] Alexander Genz (n 17) 47; Emmanuel Pernot-Leplay, 'EU Influence on Data Privacy Laws: Is the U.S. Approach Converging with the EU Model?' (2020) 18(1) Colorado Technology Law Journal 101.

[108] On this: Daniel J Solove and Paul M Schwartz, *Privacy, Law Enforcement, and National Security* (n 60) 7.

speech:[109] For example, the renowned legal scholar *Solove* argues for its greater consideration in the area of data protection[110] – and in practice, too, some government surveillance and search measures or information collections have points of contact with the areas protected by the US Constitution 1st Amendment.[111]

However, this continues to be countered by the weighty argument that ultimately any law restricting data processing could be measured against freedom of speech (problem of the paramount importance of the 'Freedom of Speech').[112]

b) State Constitutional Law

In some states the protection of privacy is guaranteed qua constitution:[113] This is, for example, in

- Alaska (Alaska Constitution, Art I § 22),
- Florida (Florida Constitution, Art I § 23),
- California (California Constitution, Art I § 1 – this article does not only apply to public agencies but even to private entities[114]).

4. Statutory Law – at the same time: Differentiation of Public and Private Sector

At the level of statutory law, a distinction must be made between the law that addresses state agencies or the public sector (see a) below) and the law that addresses private actors (see b) below). It will become apparent that the financial sector probably has the greatest density of provisions to protect the confidentiality of private data.[115]

The function of existing data protection laws is typically to ensure that the private individuals concerned have some control over their data.[116]

a) Law Addressing State Agencies respectively the Public Sector

With regard to the numerous legal acts that address the state authorities, respectively the public sector, a distinction must further be made between the federal level (see aa) below) and the level of the individual states (see bb) below).

aa) Federal Statutory Law

(1) Privacy Act

The Privacy Act of 1974, as a legislative reaction to the Watergate affair[117], is the first nationwide regulation to protect private individuals against sovereign interventions into their privacy.[118] It was originally intended to be an omnibus bill, but was subsequently limited to federal agencies based on a balance of interests and risks.

(2) Privacy Protection Act

Furthermore, the Privacy Protection Act of 1980 – an statutory manifestation of the US Constitution 1st Amendment mentioned above (see C.I.3.a)bb)) – should also be noted on the federal level.

---

[109] Alexander Genz (n 17) 48; Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 34 with further references.

[110] Daniel J Solove and Paul M Schwartz, *Privacy, Law Enforcement, and National Security* (n 60) 103 et seq.

[111] ibid 95 et seqq.

[112] *Virginia State Board of Pharmacy v Virginia Citizens Consumer Council, Inc.* 425 US 748 (1976); confirming: *Sorrel v IMS Health, Inc.* 564 US 552 (2011); On this: Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection (n 18)*309 et seqq.

[113] Manfred Weber (n 85) 182, 188; Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 36.

[114] Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 36.

[115] Alexander Genz (n 17) 55.

[116] Albrecht Funk, 'Öffentlichkeit und Privatheit im Zeitalter technischer Kommunikation: Ein Vergleich amerikanischer und deutscher Regelungsstrukturen' (1994) 22(4) Leviathan 560, 575.

[117] Alexander Genz (n 17) 51.

[118] ibid 50.

(3) Further Statutes

Further general regulation concerning collection of data by public authorities are

- the Federal Wiretap Act, 18 U.S.C. §§ 2510(2), 2511(2)(c) (interception of non-public conversation),
- the Federal Privacy Act 5 U.S.C. § 552a(e)(7)[119] (legitimacy of public video surveillance in law enforcement),
- the Computer Matching and Privacy Protection Act (CMPPA)[120] (comparison of data), and
- the Driver's Privacy Protection Act (DPPA)[121] (the handling of personal information by the Departments of Motor Vehicles).

Specific statutes concerning the access to data by the public authorities in the field of finance[122] are

- the Bank Security Act and
- the Right to Financial Privacy Act.[123]

Isolated regulations concern identity theft ('Identity Theft Statutes'),[124] such as the Identity Theft Assumption and Deterrence Act. In addition to the (more prominent) legal 'examples' mentioned, there are also numerous other (more specific) regulations;[125] there are even those regulations that are no longer mentioned even in the broadest summarising essays.[126]

Some US authors also argue for the application of property law to data protection.[127]

bb) Statutes of the Individual States

The Privacy Protection Act mentioned above (C.I.4.a)aa)(2) above) only applies to federal authorities.[128] Other 'state treaty-like'[129] overarching regulations for the individual states are not apparent.

In order to protect privacy, the US states have enacted laws in various contexts that apply to the public and private sectors and to data sets in various areas of life.[130]

- In Illinois, the 'Illinois Biometric Information Privacy Act' of 2008 is one of the most significant laws in the field of privacy;[131]
- California[132] has particularly strict data protection legislation which leads other states to frequently follow the Californian regulation ('California Effect').[133] Accordingly, the California Consumer Privacy Act[134] (CCPA) was

---

[119] Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 685 et seqq.

[120] ibid 705 et seq.

[121] ibid 681 et seqq; Alexander Genz (n 17) 55 et seq.

[122] Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18)130 et seqq.

[123] Alexander Genz (n 17) 55.

[124] On this: Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 134 et seqq.

[125] With numerous other examples ibid 38 et seq.

[126] cf only: Alexander Genz (n 17) 50.

[127] Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 145, 197 et seqq.

[128] Alexander Genz (n 17) 51.

[129] Translated from German, 'staatsvertragsähnlich'.

[130] Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 39.

[131] On this ibid 40, 306 et seqq.

[132] Government of California, Privacy Policy <https://www.ca.gov/privacy-policy/> (last accessed on 18 November 2021).

[133] cf only Alexander Genz (n 17) 74; Manuel Klar, 'Die extraterritoriale Wirkung des neuen europäischen Datenschutzrechts' (2017) 41(9) Datenschutz und Datensicherheit 533; on this also: Jordan M Blanke, 'Protection for "Inferences Drawn:" A Comparison between the General Data Protection Rule and the California Consumer Privacy Act' (2020) 1(2) Global Privacy Law Review 81; with further reference to concrete norms: Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 145 et seq.

[134] Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 129, 302 et seqq; Mathias Lejeune, 'Der California Privacy Rights Act (CPRA)' (2021) 9(1) Privacy in Germany 25.

already a 'far reaching privacy law'[135]. Other significant standards are

- The Confidentiality Medical Information Act[136],
- California's Financial Information Privacy Act, Cal. Fin. Code §§ 4050–4060[137], and
- the Penal Code, §§ 630 et seqq (PC);
- Vermont is known for its 'opt-in-approach'.[138] Also noteworthy is the ruling in Sorrell v IMS Health Care Inc;[139]
- Virginia has the 'Virginia Consumer Protection Act'.[140]

Concluding remarks: Recently, unifying data protection laws for the consumer sector have followed in various states – in quick succession. The International Association of Privacy Professionals' (IAPP) and the National Conference of State Legislatures' (NCSL) summaries provide a good overview:
- US State Comprehensive Privacy Law Comparison[141]
- 2020 Consumer Data Privacy Legislation[142]
This development should be kept in mind. – It allows (almost) to hope that a more comprehensive approach to the problem could also become possible in other areas of US data protection.

b) Law Addressing Private Actors

The sector-specific US data protection law for private economic actors – see C.I.6. below for more details – only addresses very specific privacy interests, which it locates, for example, in the following market areas or concrete relationships between providers and consumers:[143]

aa) Financial Services

The regulation of financial services includes in particular the following two laws which have been frequently received:

- Firstly, the Fair Credit Reporting Act[144] (FCRA) to protect information collected by consumer reporting agencies in order to be able to make statements about credit scores – and
- the Gramm-Leach-Bliley Act (GLBA)[145] to protect the processing of bank data.

Moreover, the following acts are noteworthy in the area of financial services:

- The Electronic Fund Transfer Act[146],
- the Equal Credit Opportunity Act,
- the Fair and Accurate Transaction Act, and
- the Fair Credit Biling Act.

---

[135] Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 40 with further references.

[136] Alexander Genz (n 17) 74.

[137] Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 128.

[138] ibid.

[139] Paul M Schwartz and Karl-Nikolaus Peifer (n 23) 134.

[140] Summing up current developments, see Axel Spies, 'USA: Neues Datenschutzgesetz im US-Staat Virginia' (2021) 3 ZD-Aktuell 05047.

[141] Taylor Kay Lively, 'US State Privacy Legislation Tracker' (iapp, last updated 7 April 2022) <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/> (Last accessed 8 April 2022).

[142] National Conference on State Legislature, '2020 Consumer Data Privacy Legislation' <https://www.ncsl.org/research/telecommunications-and-information-technology/2020-consumer-data-privacy-legislation637290470.aspx> (Last accessed 8 April 2022).

[143] Paul M Schwartz and Karl-Nikolaus Peifer (n 23) 136.

[144] Fair Credit Reporting Act, 15 U.S.C. §§ 1681 et seq, <https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act> (last accessed 18 November 2021); Alexander Genz (n 17) pp 60 et seqq; Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 87 et seqq; Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 755 et seqq.

[145] Alexander Genz (n 17) 63; Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 124 et seqq; Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16), 792 et seqq.

[146] Alexander Genz (n 17) 62 et seq.

Against the background of the laws oriented towards banking and the 'small' consumer, it remains to be seen whether data protection will soon increasingly focus on the ever 'bigger fish' – ie private financial managers – especially 'BlackRock' and 'Vanguard': At the latest since the startling collapse of the last major real estate financial bubble in 2007/2008 and the accompanying banking crisis, they have not only taken on bank-like functions due to the huge increase in private assets to be managed, but have also gained insight into huge amounts of data through modern 'market analysis tools'[147], while transparency in the use of the collected data – also in light of possible 'common-ownership' links[148] that cast doubt on any well-intentioned 'Chinese Wall' – does not always seem to be guaranteed.[149]

bb) Data Protection in Media Regulation

Regarding data protection in context of media regulation some statutes are (particularly) relevant:

(1) **Media in General**

- Cable Communications Policy Act[150]
- Communications Act[151]
- Video Privacy Protection Act[152]

(2) **Telecommunication and New Media**

- Children's Online Privacy Protection Act[153]
- Digital Telephony Act[154]
- Electronic Communications Privacy Act[155]
- Telephone Consumer Protections Act[156]

cc) Data Protection and Health Care[157]

Notable in the area of health care are

- in particular the Health Insurance Portability and Accountability Act[158], but also
- the HIV Notification Statutes[159].

bb) Contract Law

Lastly, (legally) contractual arrangements are discussed in the private sector.[160]

5. Public or Private Sector as a Role Model for Regulation

An explicit role mode function of one of those factors is, *prima facie*, not recognisable.

6. General or Sector Specific Regulation

While the European GDPR takes a path that is almost 'exuberant' in terms of prevention efforts and, with its broad scope of application, also binds many small and medium-sized data processors through numerous provisions and thus ensures a high general standard of protection, it is rather characteristic for the US that regulations for the elimination of very specific problem situations are set quasi 'reactively' only in

147 cf Heike Buchter, *BlackRock: eine heimliche Weltmacht greift nach unserem Geld* (Campus Verlag 2020).

148 On (German) competition law instructive: Natalie Seitz, *Common Ownership im Wettbewerbsrecht* (Nomos 2020) 22 et seqq.

149 cf only Jens Berger, *Wer schützt die Welt vor den Konzernen?: die heimlichen Herrscher und ihre Gehilfen* (Westend 2020).

150 Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 256 et seqq.

151 ibid 253 et seqq.

152 ibid 239 et seqq.

153 ibid 258 et seqq ; Alexander Genz (n 17) 68 et seqq.

154 Alexander Genz (n 17) 67 et seq.

155 ibid 66 et seqq; Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 273 et seqq; Daniel J Solove and Paul M Schwartz, *Privacy, Law Enforcement, and National Security* (n 60) 109 et seqq.

156 Alexander Genz (n 17) 68; Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 291 et seqq.

157 Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 497 et seqq.

158 ibid 531 et seqq.

159 ibid 526 et seqq.

160 Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 184 et seqq.

particular risk situations – and often only after an acute danger has already materialised (on the background A.II.1. above).

This approach is repeatedly referred to as the *sectoral approach*[161] and is distinguished from the (broad) European *omnibus approach*.[162] This sectoral mode applies above all to the private sector of data protection, which is shaped by economic actors and for which there is 'no overarching legal framework'[163] (entirely in the sense of 'law and economics')[164] but also, for example, to the area of 'health data' that is regarded as particularly sensible in Europe (cf only GDPR, Art 9(1)).[165]

7. Self-Regulation and Data-Protection

It corresponds to the logic of this sector-specific legislation that (economic) 'self-regulation' in US data protection is prior to state regulation – and that the latter only fills in (as a substitute) when the 'invisible hand' of the market (which is sometimes blind to justice), which is primarily concerned with wealth-creating growth (see A.II.1. above), does not adequately deal with security problems that arise – as sufficiently proven by the concrete consequences of insufficient standards in the area concerned.

Thus, self-regulation[166] becomes a central basis especially in US consumer data protection:

The companies can demonstrate through appropriate standards that they comply with rules in the initially largely 'non-regulated' space of the internet by disclosing whether and when or how they collect (which) data, how they treat stored data, etc. The immediate advantage for the companies disclosing themselves in this way is that they basically retain a high degree of flexibility while consumers are nevertheless guaranteed a certain degree of protection since violations of the self-inflicted rules can be prosecuted by the FTC and punished as unfair business practices.[167]

In view of these advantages and the resulting popularity of privacy standards to date, some authors argue that this form of specific 'self-regulation' – instead of generally binding federal or state laws – should be expanded even further.[168]

Notable self-regulatory standards with reference to data protection or privacy are, among others:

- the mandatory requirements under the FTC's 'COPPA Safe Harbor Program',[169] such as

---

[161] cf only: Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 810 et seq.

[162] The fact that numerous general federal laws of the United States are incorporated into the 'United States Code' (U.S.C.), which could be regarded as a comprehensive ('omnibus') codification, does not change this fundamental finding, since the U.S.C. is in fact only a purely formal 'omnibus' codification – and in this respect extends far beyond the boundaries of data protection and information law – which strings together numerous areas of law by mere 'paragraphs of order' – similar to a 'collection of laws' in Germany (such as the classical Schönfelder – now Habersack – for German civil and criminal law of the federal government).

[163] Translated from German, 'übergreifender gesetzlicher Rahmen'.

[164] Manfred Weber (n 85) 189; see also: Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 142; Paul M Schwartz and Karl-Nikolaus Peifer (n 23) 135 et seq.

[165] cf for this matter: Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 530.

[166] Instructive on self-regulation: Alexander Genz (n 17) 85 et seqq.

[167] Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 811.

[168] ibid 814 et seq.

[169] Safe Harbor Program, <https://www.ftc.gov/safe-harbor-program> (last accessed on 18 November 2021).

- the 'Internet Keep Safe Coalition' (iKeepSafe),[170]
- the 'kidSAFE Seal Program',[171]
- the PRIVO-'Privacy Assurance Program',[172]
- the 'Self-Regulatory Program for Children's Advertising'[173], and

the TRUSTe-'Children's Privacy Certification Standards';[174]

- the privacy standards of the 'Digital Advertising Alliance' (DAA)[175] in the field of e-commerce;
- the code of conduct of the 'Network Advertising Initiative' (NAI);[176]
- the (internal) standards of the 'Online Privacy Alliance' (OPA) for its members;[177]
- the standards within the 'Vendors Privacy Program' (VPP)[178]; and of course also
- internationally approved programmes for self-regulation such as the 'Cross-Border Privacy Rules' (CBPR) of the 'Asia-Pacific Economic Cooperation' (APEC).[179]

8. Underlying Principle of the Regulations

In contrast to the European data protection law's approach, the US legal regime assumes a fundamental freedom and accessibility of the (in the modern information society quasi 'torrential') flow of information (for its background, see A.II.1. above) and thus permits the processing of all personal information unless explicitly provided otherwise in one of the scattered laws (see only C.I.1. above).[180]

Furthermore, as far as more specific core principles are concerned – in Europe, for example, data minimisation or purpose limitation – there are no general provisions for the handling of personal data which further

---

170 iKeepSafe, <https://www.ftc.gov/system/files/attachments/press-releases/ftc-seeks-public-comment-ikeepsafes-proposed-safe-harbor-program-under-childrens-online-privacy/ikeepsafeprogramapp_0.pdf> (last accessed on 18 November 2021).

171 KidSafe Seal Program, Certification Rules, <https://www.ftc.gov/system/files/attachments/press-releases/ftc-approves-kidsafe-safe-harbor-program/kidsafe_seal_program_certification_rules_ftc-approved_kidsafe_coppa_guidelines_feb_2014.pdf> (last accessed on 18 November 2021).

172 PRIVO, Revised Seal Program, <https://www.ftc.gov/system/files/attachments/press-releases/revised-childrens-online-privacy-protection-rule-goes-effect-today/130701privosafeharbor.pdf> (last accessed on 18 November 2021).

173 Childrens advertising review unit, CARU`s Request for Comission Approval of Continuance of Safe Harbour Status, <https://www.ftc.gov/system/files/attachments/press-releases/revised-childrens-online-privacy-protection-rule-goes-effect-today/130701carusafeharborapp.pdf (last accessed on 18 November 2021).

174 TRUSTe, Children's Privacy Certification Status, <https://www.ftc.gov/system/files/attachments/press-releases/ftc-approves-modifications-trustes-coppa-safe-harbor-program/truste_childrencertstandards_031017.pdf> (last accessed on 18 November 2021).

175 DigitalAdvertisingAlliance, <https://digitaladvertisingalliance.org/> (last accessed on 18 November 2021).

176 NAI Code of Conduct, <https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf> (last accessed on 18 November 2021).

177 PrivacyAlliance, <http://www.privacyalliance.org/resources/> (last accessed on 18 November 2021).

178 BBB National Programs, Vendor Privacy Program Requirements, <https://bbbprograms.org/docs/default-source/gdp-materials/programrequirements_vpp_1-25-2021f37b5ecf-8e8d-4d4d-b41f-551489c89a09.pdf> (last accessed on 18 November 2021).

179 Asia-Pacific Economic Cooperation, Cross-Border Privacy Rules System Program Requirements, <https://bbbprograms.org/docs/default-source/gdp-materials/cbpr-program-requirements-01.202124215f31-cd1f-4c3c-b9cc-772e6336dd40.pdf?Status=Master&sfvrsn=8c79601_3> (last accessed on 18 November 2021).

180 Manuel Klar and Jürgen Kühling (n 99) 215; Paul M Schwartz and Karl-Nikolaus Peifer (n 23) 135.

expands the permissible uses of data once collected.[181]

9. Privileged Areas

According to the current state of research there are no specially protected areas that have been designated as such.

Due to the sectoral (private) focus of US data protection law (generally) 'privileged' areas are only conceivable in rudimentary form anyway, since a general standard of protection is not established nor guaranteed.

However, it can be assumed – at least in accordance with the idea of the US Constitution 4th Amendment (see C.I.3.a)aa) above) – that at least the individual's personal-family and spatial sphere of retreat is particularly protected.

II. Definitions

The attempt to define the term 'data' clearly, for the first time, demonstrates the difficulty of analysing US data protection law 'across the board' due to its sectoral dispersion. The following remarks may need to be corrected after more detailed research has been carried out. For the moment, the reader may forgive the lack of depth.

For the sake of clarity, a few introductory thoughts on the notion should be prefixed:

To begin with, it should be noted that there is no uniform definition of personal data (paralleled to GDPR, Art 4(1)) in US data protection (see C.I.1. above).[182]

Moreover, with regard to the following specifics (1.-3.), it is noticeable once again that US data protection law, unlike European data protection law, does not pursue a concept related to data processing but rather a sphere-related concept regarding privacy which (from a European perspective) leaves a lot of room for imprecision in its details (on the background of the schools of thought that are influential in this respect, see A.II.1. above): Since privacy as such has been declared the 'object of protection', details concerning personal data can be kept unregulated in many cases.

A clear 'turning point' in definiteness is, in this respect, the California Consumer Privacy Act which defines 'personal information' in fine detail in Civil Code, 1798.140(o)(1). This definition is often used as a role model in legal literature – the Californian law goes far beyond what is usually guaranteed by federal and state law and is similar to the concept of the GDPR.[183]

1. (Personal) Data as Object of Protection

(situational [spoken words etc.]; local/spatial [at home]; logical ['spheres']; informational [datum, information]; treatment of public or publicized data; limitations and expansions of notions; categories).

The regulations seen so far do not differentiate in their protective content according to situational, spatial, or logical information or data protection.

Rather, the central norms seem to be based on a pragmatic approach – all according to 'legal realism' (A.II.1. above) – which has allowed such jurisprudential fine-tuning to fade into the background as a remedy had to be found quickly in the context of an openly manifested 'data protection emergency', without having been able to create a uniformly thought-out overall system.

Against this background, the corresponding definitions seem to be rather situation-related – almost enacted 'in the heat of the moment'. They do not fit into a uniformly thought-out and detailed – 'mechanical' (see A.II.1. above) – overall system on an abstract level but rather encircle a concrete (dangerous) situation in a practical manner by primarily linking to actual elements that (typically) are at the addressee's hand. Thereby, they are oriented (without

[181] Emmanuel Pernot-Leplay (n 107) 38; Manfred Weber (n 85) 189.

[182] ibid 37.

[183] Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 302; Daniel J Solove and Paul M Schwartz, *Information Privacy* Law (n 16) 973.

dogmatic depth) towards the concrete circumstances.

2. Allocation of Data to a Person

(creation; possession/control; personal connection; differentiation between domestic and foreign nationals; treatment of multi-referential data; Limitations and expansions of notions; categories)

It seems that the relevant regulations do not assign data to a specific person but simply grant rights to the (potentially) data subjects whose (personal) information is available at a certain location – by way of an, so to speak, 'indirect assignment'.

With regard to the 'reference to persons', it is noteworthy that in some central laws the regulatory approach of 'Personally Identifiable Information' (PII) is used in definitions by referring to 'individual identifiability' – such as for the GLBA, 15 U.S.C. § 6809(4), or HIPAA, 45 C.F.R. § 160.103.[184] However, even for this identifiability there is no uniform use which US legal scholars 'lament'.[185]

When privacy laws do not even tie in with PII even broader differences in connecting factors emerge:

For example, the Privacy Act in § 552a(a)(4) defines a 'record' as a collection of information that has a (certain) reference to persons, while the Fair Credit Reporting Act in its § 603 – quite similarly – refers to a 'consumer report' that also contains data about a consumer. In this way, these laws do not make the data itself the subject of regulation but rather a certain type of its administration which has the consequence that the corresponding data does not have to be more precisely conceptualised.

In a similar way, HIPAA or the Federal Communications Act, for example, leave, without hesitation or constraint, extensive room for conceptual ambiguity if they can limit their protection to only certain information (and thus do not have to provide a general definition), cf 'Protected Health Information' or 'Customer Propriety Network Information' (CPNI).[186]

The Illinois Biometric Information Privacy Act of 2008 is symbolic in this respect as its definition simply covers all biometric information that could be used to identify a person.[187]

> A distinction between nationals and foreigners is not apparent.
>
> Other details are also not yet clear.

3. Reception and Recipient

(special regulation for non-profit/non-commercial actors; the public as a [legal] recipient; use of public data; specialised/special obligations for small and medium-sizes enterprises (SMEs); differentiation between recipients and third parties [especially within company groups]; differentiation between national and international actions; outsourcing options)

> Specific details about 'Reception and Recipient' could not be identified

III. Relationship between Discloser and Recipient

> It should also be noted for this report that the sheer amount of the American data protection laws has so far only allowed for a 'rough' evaluation. Whether there are further noteworthy examples of the following categories of regulation will only be revealed – possibly – by future research (within the research project).
>
> However, it is already (with sufficient certainty) clear at this point that it will not be possible to find an equivalent in US data protection law for every detail of the typical data processing process – which will be depicted below according to various levels of consideration – that

[184] Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 534.

[185] ibid 820: 'Given PII's importance, it is surprising that information privacy law in the United States lacks a uniform definition of the term'.

[186] ibid 534 et seq.

[187] On the definition of biometric information, see Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 306.

was thought of while designing the European data protection standard of the GDPR. Last but not least, it is simply too deeply grounded in competition law-approaches which always include 'open' findings – and thereby leave a quite fundamental freedom of action untouched. This is made particularly clear by regulations with abstract descriptions (of conceivable infringements) as it is known in Germany from the law of fair competition (Sec 3(1) of the Act against Unfair Competition (UWG)); see only the Federal Communications Act, which prohibits so-called 'unjust and unreasonable practices', 47 U.S.C. § 201(b). (The enforcement of data protection under Sec 5 of the Federal Trade Commission Act by the FTC, which after all remains an agency originally arising from the field of liberal economic supervision, is very similar to this approach.[188])

At some points it will become apparent that the California Consumer Privacy Act (CCPA) which exceeds many federal laws in its requirements – as already indicated – comes closest to the model of the European comprehensive context of guarantees.[189]

1. Provisions for Disclosure

(Does regulation exist? personal data as intellectual property and commercial good; data law as a framework for action; 'informational self-determination')

(In particular, general) provisions for disclosure are not apparent.
According to the current state of research it is not evident that personal data are (or can be) traded as intellectual property. However, in view of the characteristic liberality of US data protection and the aforementioned fundamentally free flow of information (C.I.8.), the assignment of such a legal position (that can be de facto seen as property-law) would also appear to be rather an 'alien to the system'.

With regard to US data protection, 'informational autonomy' is assumed to be equivalent to 'informational self-determination'.[190]

a) Disclosure Prohibitions

(protections of secrecy; multi-referentiality; disclosure to actors abroad; public communications)

There are isolated 'Evidentiary Privileges' regarding certain data, particularly in the case of requests for access to medical information;[191] but spouses, priests, and lawyers can all be covered by the 'Privacy Protection in Evidence Law'.[192]

b) Disclosure Obligations

(identification obligations and prohibition of anonymity; Tax and other control)

Anonymity is fundamentally protected by the US Constitution 1st Amendment's freedom of speech, see C.I.3.a)bb) above.[193]
Journalists, too, are generally not required to disclose anything about their sources – according to the 'reporter's privilege'.[194]

According to so-called 'HIV Notification Statutes' – in particular N.Y. Pub. Health L. § 2130 is dominant in relevant summaries – a positive HIV diagnosis together with the information identifying the person concerned must be reported to the health authorities.[195]

Such 'mandatory reporting laws' also exist in other constellations within the heath sectors (at least for particularly dangerous constellations or such that are dangerous to the public) – for example, concerning wounds inflicted by knifes or the use of weapons, and highly contagious diseases.[196]

[188] Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 922 et seq., 1043 et seq.

[189] ibid 970 et seq.

[190] Albrecht Funk (n 116) 575.

[191] Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 499 et seqq.

[192] ibid 33.

[193] ibid 248 et seqq.

[194] ibid 260 et seqq.

[195] ibid 526.

[196] ibid 529.

c) Voluntary Disclosure

(protection in dependency and hierarchy contexts; access to alternatives; prohibition of coupling; (voluntary) commercialization of personal data; incentives to data disclosure and protection therefrom [protection of adolescents; competition law; nudging]; prerequisites for consent; 'privacy fatigue'; peer pressure [eg WhatsApp])

In COPPA, according to 15 U.S.C. § 6502(b)(1)(A)(ii), the protection of minors is generally based on parental consent.

Moreover, voluntariness seems to be inherent in the liberal American legal system (cf A.II.1. above).

2. Recipient Obligations

a) Requirements for Personal Data Reception

(Information; requirements concerning content and formalities; warnings; notifications; assurances)

Informing (internet) users about data processing carried out – that concerns them – is not a fundamental obligation: privacy notices are always required when they are expected in a particular regulatory context, cf COPPA, 15 U.S.C. § 6502 (b)(1)(A)(i).

The requirement of consent is often mentioned – sometimes also under special formal requirements (especially in written form). However, for the 'free flow of information' (already mentioned under C.I.8. above) such consent is not a general requirement.

b) Obligations Concerning Received Personal Data

(purpose dedication/limitation; technological and organisational measures; data security; deletion and retention; further transmission and limitations thereto, also concerning transmission abroad)

A purpose limitation, for example, is stated explicitly in COPPA, see 15 U.S.C. § 6502(b)(2)(C).

The law is also precise from a data security perspective: 15 U.S.C. § 6502 (b)(1)(D) imposes a duty to ensure the confidentiality, security, and integrity of collected data.

A 'duty to transfer data' to public authorities in legal proceedings can be found in the Cable Communications Policy Act, 47 U.S.C. § 551(h).

In the medical field, however, there are some 'data transfer restrictions' to be considered when it comes to the confidentiality of medical information: as a rule, an explicit consent ('authorisation') is required for the transfer according to general provisions[197] which are sometimes repeated or specified in specific laws (among others by 45 C.F.R. § 164.512).[198]

In a very similar manner, this is provided for in the 'Video Privacy Protection Act' which stipulates an 'opt in for disclosure' rule – and thus, in principle, requires express written consent for disclosure.[199]

3. Discloser Control

a) Transparency and Right to Request Information

The California Consumer Privacy Act (CCPA) contains a right of access that enables consumers to be informed of all data collected about them – within the last 12 months – and the purposes of processing of such data; it also stipulates that data subjects must be informed of their (additional) privacy-related rights.[200]

COPPA does not go quite as far, but 15 U.S.C. § 6502(b)(1)(A)(i) and § 6502(b)(1)(B)(i) also contain certain information obligations and a right of access.

The GLBA contains an information obligation about the handling of data, 15 U.S.C. § 6803(a).[201]

---

[197] ibid 499, 537, 539.

[198] ibid 537.

[199] ibid 908 – there also on exceptions of this principle.

[200] ibid 971.

[201] ibid 793.

HIPAA provides that individuals must be informed of the privacy practices that apply ('Notice of Privacy Practices') and be given access to existing electronic health records upon request ('Access to Electronic Health Records').[202]

Most states have 'Patent Access Laws' in the health sector.[203]

The Illinois Biometric Information Privacy Act requires personal notification about information collected.[204]

b) Co-Determination and Co-Decision Concerning Data Use

(restrictions for use; reservation of consent; revocation of consent; contestation and objection; special rules for international contexts; technical requirements for the act of permission/consent)

From a – required – consent itself, corresponding restrictions can probably result in all areas of data protection. However, the corresponding universally valid handling is not yet apparent.

A 'right to opt out' if data is (or should be) transmitted to third parties is included in the CCPA.[205]

For information handled and stored under HIPAA, there is a 'right of amendment' and a 'right to file a complaint'.[206]

c) Revocation

(Data portability; deletion; 'right to be forgotten / to forget')

A 'Right to Data Portability' is explicitly included in the CCPA.[207]

This special legal act also contains a data subject's right to deletion ('right to have businesses and their service providers delete their personal information').[208] The automatic 'obligations to delete' described below (C.IV.1.e)) must be distinguished from this.

COPPA also contains a right to deletion: 15 U.S.C. § 6502(b)(1)(B)(ii).

d) Procedural Aspects

(costs for and effectivity of the rights of the affected persons [information, etc]; consumer appropriateness)

No really meaningful indications could be found in the individual laws on the costs and effectiveness of the control possibilities. In the cases in which the FTC enforces the respective interests of the affected parties certain regularities can be determined (cf also C.IV.2.c) below). Deadlines or even an obligation to take action cannot be inferred from the FTC Act, at least *prima facie*[209]; hence, further research must be carried out on this.

4. Enforcement

Overall, it can be stated for the enforcement described below – even if the substantive data protection law outlined above is by all means incomplete and does not in all areas offer 'adequate protection' (at least when viewed from a spoiled European perspective) – special instruments – such as punitive damages or class actions – and the (in part) very high dispute values offer facilitated and particularly powerful forms of defence.

Against this background, it can be stated: If shots are fired in the fight for justice for data subjects in US data protection, they are fired sharply.[210]

---

[202] ibid 538.

[203] ibid 530.

[204] ibid 974.

[205] ibid 971.

[206] ibid 538.

[207] ibid 971.

[208] ibid

[209] cf Daniel J Solove and Woodrow Hartzog, 'The FTC and the New Common Law of Privacy' (2014) 114(3) Columbia Law Review 583, 610.

[210] cf on this: Kenneth A Bamberger and Deirdre K Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (Amsterdam University Press 2015).

Nevertheless, the existing data protection regime seems to suffer from 'uncompensated victims'.[211]

a) Damages and Compensation

([material and immaterial] damages; reparations; disgorgement of profits; punitive damages)

In the following section, the structure and some specifics of US tort law will be presented as far as it seems relevant for data protection. Regarding 'profit forfeiture', no significant findings have been recorded so far.

aa) Damages – Generalities

An essential basis of American law to claim for compensation and damages – also in the area of data protection – is tort law.[212] It gives rise to central bases for claims (see below (1)) which aim at – material and immaterial – damages (see below (2)).

(1) Tort Bases for Claims for Damages (Privacy Torts)

These statutory bases for claims can always be attributed to one of the following four categories (i)-(iv) which are recognised and implemented in most American states today.[213] They go back to the legal scholar *William L. Prosser*[214] and are central to the means of legal protection in the area of privacy.

Violations of data protection regulations do not automatically constitute one of these 'Privacy Torts'.

> It must therefore always be examined for each individual case whether a tort category is fulfilled. Only a vague framework of the individual tort categories is outlined here. However, corresponding and more detailed information can be found in the footnotes attached to the headings. When it comes to the prosecution of unauthorised disclosures of information in the area of 'medical treatment', there are further specific guidelines that follow from concrete court decisions.[215]

(i) Public Disclosure of Private Facts / Private Matters[216]

First of all, possible 'libel'[217] is counteracted by ensuring protection against the publication of facts – even if they are actually true – if and to the extent that they are 'disparaging' and can thereby damage a person's 'good reputation'.[218]

- A significant court decision on this group of cases was issued by the Supreme Court of California: *Taus v Loftus*, 151 P.3d 1185 (2007).
- But a more recent decision of the Supreme Court of the United States is also worth mentioning – *Boring v Google*, 38 Media L. Rep. 1306 (2010) – in which the plaintiffs' challenge of a collection of material for Google Street View was rejected.

(ii) Intrusion Upon Seclusion[219]

Furthermore, a certain 'protection against curiosity' is maintained by prohibiting the

---

[211] Robert L Rabin, 'Perspectives on Privacy, Data Security and Tort Law' (2017) 66 DePaul Law Review 313, 323.

[212] Alexander Genz (n 17) 81 et seqq; Manuel Klar and Jürgen Kühling (n 99) 179; Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 136 et seqq, 144, 175 et seqq; Alexander H Tran, 'The Internet of Things and Potential Remedies in Privacy Tort Law' (2017) 50(2) Columbia Journal of Law and Social Problems 263, 279 et seqq.

[213] Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 33.

[214] William J Prosser, 'Privacy' (1960) 48(3) California Law Review, 383.

[215] On this: Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 505 et seqq.

[216] ibid 33; Robert L Rabin (n 211) 325 et seq; Alexander H Tran (n 212) 281 et seqq.

[217] Translated from German, 'Rufschädigung'.

[218] Specifically on data of patients in health care context: Daniel J Solove and Paul M Schwartz *Information Privacy Law* (n 16) 505 et seqq.

[219] ibid 89 et seq.; Robert L Rabin (n 211) 326; Alexander H Tran (n 212) 290 et seqq.

invasion of a person's privacy, such as through telecommunication surveillance or the reporting of (private) incidents such as accidents or injuries.[220]

(iii) Publicity which Places a Person in a False Light in the Public Eye[221]

This defamation-like group of cases is also very close to the 'defamation torts'[222] and, simultaneously, demonstrates their extension: Potentially affected persons are protected from the publication of false facts which, although not defamatory, are nevertheless capable of putting the 'person dragged in the mud' in a false light in the public eye.

- Worth mentioning is the Supreme Court of Ohio's decision *Welling v Weinfeld*, 866 N.E.2d 1051 (2007).

(iv) Approbation of One's Name or Likeness[223]

Alien personal characteristics shall not be used without permission by other persons for their own selfish purposes. In this way, an 'economic exploitation' of privacy is protected to a certain extent – the only materially protected good of the privacy torts.

- Significant is the Supreme Court of Colorado's decision *Joe Dickerson & Associates, LLC v Dittmar*, 34 P.3d 995 (2001).

(2) Individual Matters of (Material and Immaterial) Damage

Whether the respective privacy torts are intentional, negligent, or strict liability torts is largely determined by case law.

The differentiation is decisive for the extent of liability in individual cases:

- In the case of intentional torts, in principle, full reparation[224] are paid, whereby an injury to another's interests is sufficient and the damage incurred does not need to have been foreseeable.[225]
- In the case of negligent torts, there must firstly be causation (equivalent to a *conditio sine qua non* formula or 'but for'-rule) and secondly the damage must have been foreseeable and probable.[226]

The 'data protection tort law' of the US does not fit the traditional legal infringement categories, which are linked to quantifiable financial damages or physical impairments:[227] because there is often no clear 'material' damage that could be compensated for in the sense of the compensation principle ('compensatory damages'), which is intended to put those affected in exactly the same condition as they were in before the legal infringement,[228] cf for Germany German Civil Code (BGB), Sec 249(1).[229] Rather, the 'nominal damage' is usually relevant: in order to take account of the infringement of the plaintiff's interests, a purely symbolic amount is awarded to the affected parties.[230]

---

[220] Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 528 et seq.

[221] cf in depth: ibid 206 et seqq.

[222] Even before the 'tort law' there was the 'law of defamation' which is very similar to the data protection-related categories of tort law outlined here, cf Peter Hay (n 40) 162 et seqq.

[223] Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 220 et seqq.; Robert L Rabin (n 211) 326 et seqq.

[224] Translated from German 'unbegrenzte Totalreparation'.

[225] Peter Hay (n 40) 153.

[226] ibid 157 et seq.

[227] Woodrow Hartzog and Daniel J Solove, 'The Scope and Potential of FTC Data Protection' (n 28) 2277 et seqq.

[228] Ulrich Amelung (n 17) 257; Peter Hay (n 40) 169.

[229] Cedric Vanleenhove, *Punitive Damages in Private International Law: Lessons for the European Union* (Intersentia 2016) 9 et seqq – also there on the following sentences.

[230] Peter Hay (n 40) 168. cf also on this: Charlotte A Tschider (n 89) 52.

However, this amount does not need to be small by any means (see also C.III.4.b)dd) below).

bb) Punitive Damages

In addition to 'normal' damages which are characterised by the civil law idea of compensation for concretely suffered damage to legal positions, in the US there are also so-called punitive damages. Punitive damages have – in this respect: *nomen est omen* – above all a *punitive* character[231] and are, thus, also intended to have a general deterrent effect.[232] Accordingly, they can award very high sums of money.[233] Nowhere is this type of compensation more widespread than in the USA – nonetheless, it was even there very controversial from the beginning.[234] The idea of punitive damages was originally conveyed from common law.[235]

In principle, the awarding of 'sanctioning' damages presupposes a particularly disrespectful or serious violation of the law – a 'special severity of blame'[236]. This is possible for all offences under tort law.[237] However, there are no examples from previous data protection practice in publications to date.[238]

b) Procedural Aspects

('threshold' for legal protection; right to initiation; burden of proof and evidentiary privileges; dispute value; 'small claims'; alternative dispute resolution; rights to bring/press charges; 'rational apathy')

So far, there is nothing to report on rights to press charges and 'rational apathy'.

aa) General Procedural Aspects

In general, it can be stated that proceedings initiated by individuals begin with a lawsuit – which is usually filed in accordance with Rule 3 of the Federal Rules of Civil Procedure (FRCP) or in accordance with the specifications stated there.

Regarding the bearing of costs, the so-called 'American Rule' applies according to which, as a matter of principle, each party has to bear its own legal costs and attorney's fees.

In exceptional cases, the law provides that the unsuccessful party must bear all costs.[239]

bb) Particulars in Enforcing Privacy Torts

In order to assert the privacy torts described above (C.III.4.a)aa)(1)), the plaintiff as such must be affected; see for this also *Uranga v Federated Publications, Inc.,* 138 Idaho 550 or *Loft v Fuller*, 408 So. 2d 619.

Tort law cases usually come before a jury court by way of civil litigation.[240]

Since the jury consisting of laymen in tort cases is often very 'plaintiff-friendly' – and since there is a 'plaintiffs' bar' where lawyers specialising in tort law can be hired under a

---

[231] Instructive for the field of media and information law: Ulrich Amelung (n 17) 265 et seqq. Peter Hay (n 40) 169 et seqq.

[232] In further depth – also regarding other functions –, Juliane Mörsdorf-Schulte, *Funktion und Dogmatik US-amerikanischer punitive damages: zugleich ein Beitrag zur Diskussion um die Zustellung und Anerkennung in Deutschland* (Mohr Siebeck 1999) 60 et seqq.

[233] cf only Lothar Determann, *Datenschutz: International Compliance Field Guide* (C. H. Beck 2017) 174.

[234] cf only Peter Hay (n 40) 70.

[235] Juliane Mörsdorf-Schulte (n 232) 180 with further references.

[236] Ulrich Amelung (n 17) 259 et seq.

[237] ibid; With the vague suggestion that under the law of some states punitive damages are to be considered in any event: Charlotte A Tschider (n 89) 52.

[238] Only cautiously hinting at the possibility of their imposition, Charlotte A Tschider (n 89) 52; For the UK, for example, an extensive empirical study was carried out in 2018 which also included statements on 'punitive damages' in the field of data protection, James Goudkamp and Eleni Katsampouka, 'An Empirical Study of Punitive Damages' (2018) 38(1) Oxford Journal of Legal Studies 90, 100.

[239] Peter Hay (n 40) 71.

[240] ibid 148.

profit-sharing agreement – tort cases usually have a good chance of success.[241]

> Formal evidence facilitations have not occurred during the research so far.

cc) Other Private Possibilities to Sue[242]

If tort law does offer a legal action, means of 'private enforcement' must be enabled by the specific data protection laws themselves in order to provide for possibilities of legal protection for (potentially) affected persons.[243]

Some laws, such as HIPPA, even explicitly exclude enforcement options for individuals.[244]

In some cases, in which individuals cannot defend themselves against an infringement of their interests, it is possible that they will be compensated by 'refunds' from the FTC.[245]

dd) Dispute Value

Data protection law in the USA is practically effective because occasionally extremely high claims for damages are granted (in the case of class actions – see below, ff) – these can reach into the millions).[246]

ee) Alternate Dispute Resolution

The two main instruments of alternative dispute resolution (also in data protection law) are mediation and mandatory arbitration.

Mediation is an attempt to reach an agreement before a body that is independent of the courts. In some states, such an effort is even obligatory in certain constellations, such as for damage claims in Florida: Florida Statutes, Sec 44.102(2) (2007). Mediation proceedings may be converted into arbitration proceedings if necessary.

'Local rules' determine whether and, if so, in which situations arbitration can or must be conducted before which court. For example, at the California Superior Court, all actions for damages up to $50,000 are subject to arbitration under Sec 1141.11 of the Code of Civil Procedure (CCP).

General details can be found in 28 U.S.C. §§ 651 et seqq. which constitute the 'Alternative Dispute Resolution Act' (1198). The final arbitral award regularly has the same effect as a formal judgment – unless one of the parties requests to benefit from a 'jury verdict' after the proceedings (so-called jury guarantee), see bb) above.

If expressly mentioned by law, mandatory arbitration can also be replaced by mediation, for example in California under Sec 1775.3 of the CCP.

ff) Class Action

By means of a class action[247], regulated in FRCP: 23rd Rule, one or more affected persons can bring a lawsuit on behalf of a group of equally affected persons. This definition already suggests that no exceptions are (or can be) made to the requirement of being individually affected (see bb) above), also in the area of collective redress, cf only *Tabata v Charleston Area Medical Center, Inc,* 233 W.Va. 512.

---

[241] ibid.

[242] With general details on (civil procedural) legal action options, ibid 49 et seqq, 68 et seqq.

[243] cf Elizabeth D de Armond, A Dearth of Remedies (2008) 113(1) Dickinson Law Review 1.

[244] Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 547.

[245] To this Federal Trade Comission, Refunds, <https://www.ftc.gov/enforcement/cases-proceedings/refunds/how-ftc-provides-refunds> (last accessed 18 November 2021).

[246] Lothar Determann, 'Datenschutz in den USA – Dichtung und Wahrheit' (2016) 35(9) Neue Zeitung für Verwaltungsrecht 561, 562, 567.

[247] Stephanie Eichholtz, *Die US-amerikanische Class Action und ihre deutschen Funktionsäquivalente* (Mohr Siebeck 2002) 29 et seqq. – there also on the historical development, 33 et seqq.

Regarding the definiteness of a class action, it must become clear whom exactly the class action concerns.[248]

While the classical main areas of application of collective redress are consumer protection and competition law,[249] a class action in data protection admittedly only comes into consideration if a 'security breach' entails a large number of privacy violations.

It is at times assumed that this form of legal protection is very common in US data protection enforcement.[250] In practice, however, it is nonetheless not easy for lawyers who are to bring class actions to demonstrate and substantiate damages as a result of a breach of personal data protection.[251]

If the law – for example in the area of 'breach notifications' (see C.IV.1.b) below) – were more standardised, class actions to enforce data subjects' rights would be considered more often.[252]

Even if a combination of punitive damages (see C.III.4.a)bb) above) and class actions is possible in special constellations, it does not seem to be the rule.[253]

IV. Objective Legal Obligations of the Recipient

1. Obligations Concerning Received Data

a) Dependence on Authorisation

(of business models, processing variants, terms and conditions)

Provisions concerning dependences on authorisation probably only refer to specific data processing operations, not to entire business models or basic processing procedures – *eg* the Cable Communications Policy Act (CCPA): 47 U.S.C. § 551(b)(1) and (c)(1).

b) Notification Duties

(regarding business models and business activities; regarding processing activities)

The most significant notification obligations in US data protection law are 'data breach notification provisions'[254] according to which data subjects must be informed if unauthorised processing or disclosure of their personal information has occurred.

Data breach notification rules are – in comparison to the 'primary' legal norms concerning the original data processing – a form of 'post-regulation' which is intended to initiate a transparent data protection competition and to encourage companies to consistently implement data protection.[255]

The data breach notifications' pioneer was, as so often in data protection matters, California, cf Cal. Civ. Code, Sec 1798.82(a); by nowadays, all states have enacted corresponding legal provisions which, in turn – see C.I.1. above – has led to a high degree of fragmentation.[256] Proposals are therefore made for greater standardisation at the federal level (cf A.I.4. above) which would allow to evaluated and summarised the individual state laws in order to optimise the affected persons'

[248] ibid 29 – on further preconditions pp 31 et seq., 77 et seqq.

[249] ibid.

[250] Lothar Determann, 'Datenschutz in den USA – Dichtung und Wahrheit' (n 246) 566; Lothar Determann, *Datenschutz: International Compliance Field Guide* (n 233) 175.

[251] On this Lothar Determann, *Datenschutz: International Compliance Field Guide* (n 233) 176.

[252] cf Charlotte A Tschider (n 89) 77.

[253] Francis E McGovern, 'Punitive Damages and Class Actions' (2010) 70(2) Louisiana Law Review 435.

[254] In more depth, see Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 345 et seqq.; Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 1013 et seqq.

[255] Robert L Rabin (n 211) 322 et seq.

[256] Detailed Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 1013 et seqq; With more accurate proof regarding individual statutes, Charlotte A Tschider (n 89) 25, 65.

protection and can finally be enforced uniformly by the FTC (C.IV.2.c) below).[257]

c) Documentation

(accountability)

The HITECH Act (2009) contains a specific HIPAA Breach Notification Rule: It states that data breaches must be documented and notified to the data subjects – see b) above.

d) Processing Requirements

(prohibition subject to permission; balancing of interests; restrictions for terms and conditions; business practices; APIs/interfaces for third parties)

So far, no concrete examples have been found.

e) Prohibitions and Obligations

(prohibition of processing variants [eg profiling]; criminal prohibitions; restrictions under competition regulations; prohibition of abuses [of power/market power]; further transmission to third parties, especially governmental bodies; elicitation from abroad)

In Pennsylvania, according to 71 Pa. Stat. Ann. § 1690, 108 – there is a prohibition regarding the disclosure of information obtained during alcohol or drug withdrawal treatment.[258]

In some statutes, 'request-independent', *ie* objective, obligations to erasure have been established: *eg* 18 U.S.C. § 2710(e) imposes an obligation to erase personal information that no longer needs to be stored; similar rules are found in the Cable Communications Policy Act, 47 U.S.C. § 551(e) as well as in the Illinois Biometric Information Privacy Act[259].

Disclosure of data to third parties or the state is initiated by 'Research Disclosure Laws' that mandate the release of health data for research purposes, such as under Sec 11977 of the Cal. Health & Safety Code.[260]

The Illinois Biometric Information Privacy Act[261] prohibits the resale of collected data.

2. Monitoring

a) Recipient Self-Monitoring

(self-restrictions; compliance mechanisms; internal responsibilities [company privacy officers; ombudspersons)

HIPAA prescribes the establishment of 'Privacy Officials' who must ensure compliance with the corresponding data protection regulations.[262]

It also stipulates that compliance standards must be documented – all employees must be trained to comply with the relevant requirements.[263]

Many (larger) companies now have a 'Chief Privacy Officer' (CPO) to safeguard their customers' and consumers' data protection. The CPO also regularly prepares a 'privacy program' that summarises compliance regulations. However, there does not seem to be a concrete threshold above which such a data protection officer must be employed.[264]

b) Regulated Self-Regulation

(sectoral and industry associations)

In the context of private data protection, self-regulation, which is also carried out by sector and industry associations, is of particular importance: Generally binding and state-initiated standards are deliberately only enacted when problems – evidentially – cannot be solved in the free market economy without legislation (see C.I.7. above).[265]

c) Supervisory Authorities

(data protection authorities; competition authorities; economic oversight authorities)

---

[257] Charlotte A Tschider (n 89) 45 et seqq, in particular 65 et seqq.

[258] Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16*)* 530.

[259] ibid 974.

[260] ibid 529.

[261] ibid 975.

[262] ibid 536.

[263] ibid.

[264] ibid 812.

[265] Hans J Kleinsteuber (n 86) 49.

In principle, the US does not have data protection authorities.[266]

Only the state of California which – as already mentioned – already has a particularly differentiated and strict substantive law (see C.I.4.a)bb) above) does also have its own 'Office of Privacy Protection'.[267]

Otherwise, the FTC, founded in 1914, which was also entrusted with significant tasks in (other) areas of the economy by the Federal Trade Commission Act[268] assumes the function of a supervisory authority in data protection[269] – at least *de facto*.[270]

The fact that an institution focused on the economic sector is the 'kind of data protection authority'[271] in the United States illustrates the private economic focus of the current data protection regime.

The FTC is responsible for almost all data protection[272] but assumes special significance in cases where there is no possibility of private enforcement for data subjects.[273]

It conducts an 'administrative proceeding'[274] which usually ends in a settlement ('Consent Agreement') with certain conditions and penalties.[275] Only after the conclusion of these proceedings at the FTC, court proceedings can be pursued.

It is noteworthy that the Federal Trade Commission, through its nationwide jurisdiction, ensures a certain 'equality of rights' through 'equal treatment' in the application of certain principles[276] and thereby makes an important contribution to the somewhat broader standardisation of data protection ('the closest thing the United States has to omnibus privacy regulation').[277] The importance of the FTC's work is often underestimated in academia, including abroad; the FTC's actions have almost led to a kind of common law in the area of enforcement.[278] Sometimes it is even assumed that this special assumption of responsibility by the FTC is indispensable for the functionality (and legitimacy) of the – materially incomplete – data protection concept of the United

---

[266] Lothar Determann, *Datenschutz: International Compliance Field Guide* (n 233) 174; Albrecht Funk (n 116) 575.

[267] Alexander Genz (n 17) p 75.

[268] See only the homepage of the FTC: <https://www.ftc.gov/about-ftc> (last accessed on 18 November 2021); Peter Hay (n 40) 255.

[269] Instructive, Woodrow Hartzog and Daniel J Solove, 'The Scope and Potential of FTC Data Protection' (n 28) 2236; Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (n 18) 200 et seqq; Daniel J Solove and Paul M Schwartz *Information Privacy Law* (n 16) 1043 et seqq.

[270] On this, Daniel J Solove and Woodrow Hartzog, 'The FTC and the New Common Law of Privacy' (n 209) 600.

[271] ibid 676.

[272] See only the first instance decision of the New Jersey Federal District Court *Federal Trade Commission v Wyndham Worldwide Corp,* (Civil Action) No 13-1887 (2014). The FTC informs on its own homepage which laws it enforces and in which areas it acts administratively: <https://www.ftc.gov/legal-library/browse/statutes> last accessed on 18 November 2021); Some data protection laws explicitly address FTC enforcement, such as COPPA under § 312.9. or § 621(a) of the FCRA.

[273] cf only Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 794, 870.

[274] cf on the exact procedure Daniel J Solove and Woodrow Hartzog, 'The FTC and the New Common Law of Privacy' (n 209) 609 et seq.

[275] The high settlement rate at the FTC means that the FTC itself can establish a kind of 'case law' in which it largely defines the relevant requirements of an '(un)fair' practice itself; this underpins its position of power, Daniel J Solove and Woodrow Hartzog, 'The FTC and the New Common Law of Privacy' (n 209) 612 et seqq.

[276] Administrative agencies such as the FTC have taken on a comprehensive regulatory function ('through the back door') in the 20th century which was once the preserve of the courts, cf Peter Hay (n 40) 5.

[277] Daniel J Solove and Woodrow Hartzog, 'The FTC and the New Common Law of Privacy' (n 209) 676; On the critiques of this powerful position, see the summary by Woodrow Hartzog and Daniel J Solove, 'The Scope and Potential of FTC Data Protection' (n 28) 2237 et seqq.

[278] Daniel J Solove and Woodrow Hartzog, 'The FTC and the New Common Law of Privacy' (n 209) 676.

States.[279] For the persisting 'black holes' in sector-specific data protection are in no way illuminated by the increasing frequency and intensity of legal violations.[280]

Accordingly, it is suggested that the FTC should be further strengthened in its unifying function in order to shape the rather fragmented data protection tangle 'into something more coherent and comprehensive'.[281]

Because specific privacy laws have been created for so many different sectors (see only C.I.1. above) there are other administrative agencies besides the FTC that oversee compliance or enforce laws in specific sectors:[282]

- In the banking sector the 'Office of the Comptroller of the Currency' (OCC) operates.
- The Securities Exchange Committee (SEC), a stock market regulator, oversees the broader capital market.
- The 'Department of Health and Human Services' (HHS) and the 'Office for Civil Rights' (OCR) provide privacy support in the health sector.[283]
- The Federal 'Communications Commission' (FCC)[284] is responsible for communications.

However, even the high level of sensitivity to a lack of competition and the consequential problems resulting from market concentrations, which should actually – due to the staffing of the relevant supervisory authorities with economic experts – also and actually arise in the handling of 'privacy protection' in practice, has not been able to prevent serious monopoly formations in the area of financial administrations (see C.I.4.b)aa) above) and digital platforms, which are (not only, but especially) worrying in terms of data protection: For example, the financial services provider 'BlackRock' has insights via 'Aladdin', its portfolio management software, into data volumes that defy any descriptions. And the digital platforms' 'Big Four'[285] have – in a very similar way – a power flowing from their big data collections that should be gated by democratic constitutional means.[286]

In this respect, it remains to be hoped for a better exploitation of the concrete market-related 'know-how' of the economic bodies entrusted with data protection in the area of supervision: If public institutions – such as the FTC and the OCC or SEC – (must) keep an eye on market developments anyway, their responsibility for privacy could also provide a motivation for better containment of potentially 'too powerful' actors.

d) (Specific) Criminal Prosecution

(focus) prosecution units for informational offences; [situational/special] investigators)

The U.S. Department of Justice often leads 'general' law enforcement in data protection.

The Consumer Financial Protection Bureau (CFPB) also receives complaints in the financial sector.[287]

---

[279] Woodrow Hartzog and Daniel J Solove, 'The Scope and Potential of FTC Data Protection' (n 28) 2267.

[280] ibid; Robert L Rabin (n 211) 313 et seq., 318, 323; Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 1011.

[281] Woodrow Hartzog and Daniel J Solove, 'The Scope and Potential of FTC Data Protection' (n 28) 2271 et seqq.

[282] ibid at. 2236; Robert L Rabin (n 211) 319. Charlotte A Tschider (n 89) 53.

[283] cf Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 554 et seq.

[284] ibid 923.

[285] Namely Amazon, Apple, Facebook, and Google – see already A.I.1. above.

[286] cf only Jans Berger (n 149); Norbert Häring, *Endspiel des Kapitalismus: Wie Konzerne die Mach übernahmen und wie wir sie zurückholen* (Quadriga 2021).

[287] Consumer Financial Protection Bureau, <https://www.usa.gov/federal-agencies/consumer-financial-protection-bureau> (last accessed on 18 November 2021).

HIPAA law is enforced by special official bodies.[288]

In privacy-friendly California, there is a 'California Attorney General' for the privacy law enshrined in CCPA.[289]

e) Procedural Aspects

(investigation powers; resources of monitoring institutions)

Based on 15 U.S.C. § 45(a)(2)[290], the FTC may issue a consent order for an external audit of a company's privacy practices by independent auditors.

3. Enforcement

a) Intervention Concerning Data Processing

(restriction and prohibition of data processing)

In the past, the FTC has already issued prohibitions against future unfair practices that have already been specifically reprimanded by the FTC, cf 15 U.S.C. § 45 (a)(2).

On this legal basis, the FTC can also oblige a company to take technical and organisational measures (to ensure sufficient data security) or to draft a comprehensive data protection concept.

As far as can be seen, there are no other data-processing-related interventions.

b) Intervention Concerning Business Models

(competition and economic supervision; government/public monopolies)

On the competition-related function of the FTC or other supervisory authorities in data protection, see already C.IV.2.c) above.

c) Penalties for Processors

(prohibition orders concerning business activities; corporate sanctions; revenue-based sanctions)

Even if it is not clear from the following legal bases that they establish 'processor-related' sanctions according to their objective, the fines mentioned here can be so high that they have a *de facto* company-related effect in any case:[291]

- Under 15 U.S.C. § 45(l), failure to comply with a final order of the FTC may result in a fine of up to $10,000 which may be collected by the Attorney General's Office. Each day of – continued – 'noncompliance' is considered a separate violation which can result in very large fines (the highest amount to date was $5 billion).
- Under 15 U.S.C. § 45(m), the FTC may bring a private action for a wilful data breach that constitutes an unfair act – see C.IV.4(a)(aa)(1) above – or a wilful violation of one of its orders, seeking a civil penalty of up to $10,000 per violation (and again: per day of 'continued violation').
- Under 15 U.S.C. § 45(a)(2), the FTC may also assess penalties in individual cases that exceed the statutory range.

It is not unusual for the FTC to impose several of these measures at once which not only increases the sanction's intensity but also its 'corporate-related' effect.

d) Penalties for Individual Actors

([managing] directors' liability; individual criminal sanctions)

The FTCA refers in every enforcement authorisation to a possible action against 'any person, partnership, or corporation', whereas

[288] Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 547.

[289] ibid 972.

[290] This norm represents a general authorisation of the FTC that is (also) significant for the enforcement level – see C.IV.3. below – in order to avert 'unfair practices of competition' that constitute specific data protection violations in relation to privacy.

[291] Arguably, something similar can be said for the Health Information Technology for Economic and Clinical Health Act (HI-TECH), which allows for higher sanctions for the scope of HIPAA, Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (n 16) 532.

in practice it always seems to be a company as such – as the processor violating data protection law *in concreto* – that becomes the addressee of the FTC's orders.

More in-depth details – with an impact on corporate law – may still need to be researched.

e) Procedural Aspects

(priority of data regulation enforcement; resources of enforcers; shaming impact/pillorying effectof breaches/violations)

The exact number of data protection cases handled by the FTC to date can be found on its homepage.[292] Whether conclusions about the 'priority' of data offences can be derived from these figures seems questionable. In any case, the complaints about the *status quo* of US data protection repeatedly voiced in legal publications suggest that the enforcement level cannot make up for the lack of consistency in substantive law, even if the FTC carries out a very important task.

The corresponding websites also provide some information on the (financial and personnel) resources and staffing of the authorities.[293] However, the specific budgets available for data protection are not (always) apparent.

> At present, no other information can be provided.

The fact that all data protection violations dealt with by the FTC (including the corresponding official written pleadings) are made publicly available on the FTC's website may have a 'pillorying effect'[294].

Similarly, if a company submits to a (private) self-regulatory association under COPPA, the respective association must publicly report all violations committed by its registered members and the actions taken against those violations, COPPA § 312.11(b)(3)(i).

D. Sources and Literature

I. Relevant Monographs

- Alexander Genz, *Datenschutz in Europa und den USA: Eine rechtsvergleichende Untersuchung unter besonderer Berücksichtigung der Safe-Harbor-Lösung* (Deutscher Universitätsverlag 2013).

II. Relevant Articles

- Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4(5) Harvard Law Review.
- Woodrow Hartzog and Daniel J Solove, 'The Scope and Potential of FTC Data Protection' (2015) 83(6) George Washington Law Review
- Daniel J Solove and Woodrow Hartzog, 'The FTC and the New Common Law of Privacy' (2014) 114(3) Columbia Law Review

III. Leading Cases

- *Olmstead v United States*, 277 US 438 (1928).
- *Katz v United States*, 389 US 347 (1967).

IV. Other Cases

- Daniel J Solove and Paul M Schwartz, *Information Privacy Law* (7th ed., Wolters Kluwer 2020) 817
- Daniel J Solove and Paul M Schwartz, *Consumer Privacy and Data Protection* (3rd ed., Wolters Kluwer 2020)

---

[292] Since 2020, the FTC has handled 30 privacy-related cases – including only 5 to date in 2021; in comparison, since 2020, the FTC has handled a total of 220 cases, including 84 to date in 2021, <https://www.ftc.gov/enforcement/cases-proceedings> (last accessed on 18 November 2021).

[293] cf for example Congressional Budget Justification Fiscal Year 2022, <https://www.ftc.gov/system/files/documents/reports/fy-2022-congressional-budget-justification/fy22cbj.pdf> (last accessed on 18 November 2021).

[294] Translated from German, 'Prangerwirkung'.