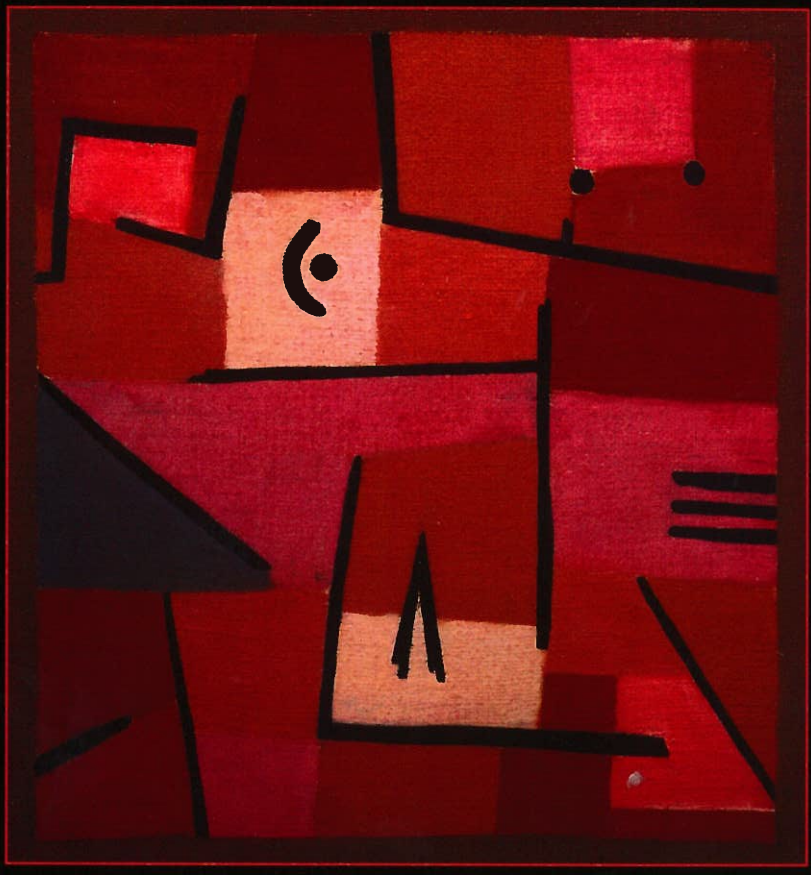
Social Dimensions of Privacy

Interdisciplinary Perspectives



Edited by

Beate Roessler and Dorota Mokrosinska

SOCIAL DIMENSIONS OF PRIVACY

Interdisciplinary Perspectives

Edited by
BEATE ROESSLER
AND
DOROTA MOKROSINSKA

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107052376

First published 2015

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing in Publication data
Social dimensions of privacy : interdisciplinary perspectives / edited by Beate Roessler and Dorota Mokrosinska.
pages cm
Includes bibliographical references and index.
ISBN 978-1-107-05237-6 (hbk)
1. Privacy, Right of – Social aspects. I. Roessler, Beate, 1958– editor. II. Mokrosinska, Dorota, 1967– editor.
JC596.S63 2015
323.44'8–dc23
2014049357

ISBN 978-1-107-05237-6 Hardback

17

The value of privacy federalism

PAUL M. SCHWARTZ

Introduction

The United States features a dual system of federal and state sectoral law. In the absence of an omnibus privacy statute, the key question is how these laws interact with each other. When Congress enacts privacy law, it generally allows the states space for further action. The federal lawmaker typically does so through laws that set only a floor, that is, a minimum of safeguards, but that allow the states to exceed their privacy protections. This model has involved a wide range of institutional actors in the regulation of privacy. State legislatures and courts interpret state laws. Congress acts to preempt state law in enacting sectoral legislation, as needed, and federal judges interpret state legislation, including subsequent amendments to existing state law or new laws, to decide if they conflict with federal law.

This existing US model is under pressure, however, because the federal government is largely inactive. The risk is that a new generation of state privacy legislation, such as breach notification laws, will not be consolidated and improved through the federal legislative process. Gridlock in Washington DC has suspended the normal process of privacy federalism.

In the European Union, the situation is different. At present, the Data Protection Directive requires member states to enact legislation that is "harmonized" around its rules for information privacy. In the resulting legal system, the focus remains on the member states, which are left with a "margin for maneuver" that permits national differences in the resulting statutes. The result has not been viewed as satisfactory due to a fragmentation of data protection in the EU. Under the Proposed Data Protection Regulation, however, there will be different concerns regarding the relationship between the member states and Community. The Proposed Regulation will be directly binding on member states and largely replace national data protection law. It will also shift power at the institutional level to the Commission and away from the member states. There is a

danger that this approach will stifle innovation and heighten the democratic deficit in the EU.

Thus this chapter will analyze two widely different kinds of privacy federalism. In the USA, there is a diffuse system in which the chief risk currently is that of too little consolidation of privacy law at the federal level. In contrast, in the EU, under the Proposed Data Protection Regulation, the chief danger appears to be from the future centralization of power in the institutions of the Union.

"Privacy federalism" is a combined term and both elements of it should be introduced at this juncture. By "privacy," this chapter generally means the legal rules for regulating the processing of personal information by organizations in the public and private sector. In the United States, this area of regulation is called "information privacy law." The similar term in the European Union and, indeed, in the rest of the world, is "data protection law." By "federalism," this chapter indicates a legal granting of partial autonomy in regulatory decision-making or specific areas of governance to geographically defined smaller units (Feeley and Rubin 2008: 22). This definition is of applicability both to the kinds of shared authority in the United States among the federal government and states, and in the European Union between the institutions of Brussels and those of the member states. Putting these terms together, this chapter uses "privacy federalism" as a reference to the different ways that legal authority for information privacy law or data protection law can be distributed among different levels of regulatory authorities, whether national or state in the United States, or European Union and member states in Europe.

US privacy federalism

This section examines the model of privacy in the sectoral system of the United States. It will analyze the laws as well as the different institutional entities involved in shaping privacy law.

Privacy federalism in a sectoral system

A patchwork of information privacy law exists in the United States. While nations in the EU have long enacted omnibus information privacy laws, the United States has promulgated only sectoral laws. An omnibus privacy law typically extends to government and private companies alike. Examples of such national laws are Germany's Federal Data Protection Act (1977) and France's Law on Information Technology, Data Files and

Civil Liberties (1978). There is no similar kind of national omnibus privacy law in the United States.

In Europe, moreover, national lawmakers typically supplement their omnibus laws with sectoral statutes. In Germany, for example, the Telecommunications Act (2004), among its other provisions, specifically regulates the collection and use of personal data in telecommunications. It has specific rules for "location-based data" (*Standortdaten*), including rules that distinguish between the use of such information for "self-location" (*Eigenortung*) and "external-location" (*Fremdortung*). The Telecommunication Act's specific provisions (2004: §§ 91–107) take precedent over the general rules in the Federal Data Protection Act. Where a specific provision is not present or there is ambiguity regarding it, the requirements of the national omnibus law are applicable.

In contrast to an omnibus law, a sectoral law regulates only a specific context of information use. Information privacy law in the USA takes precisely this approach. As examples, the Fair Credit Reporting Act (1970) contains rules for the use of credit reports, and the Video Privacy Protection Act (1988) establishes rules concerning the use of video rental information. As Daniel Solove and Woodrow Hartzog summarize: "By and large, it is fair to say that US privacy law regulates only specific types of data when collected and used by specific types of entities" (Solove and Hartzog 2014: 586). Due to the absence of an omnibus statute, the legal system in the United States contains gaps in its coverage. As a further matter, in the absence of the safety net that an omnibus law provides, one of the most critical issues for information privacy law concerns a threshold question: the applicability of any specific law. The answer to questions such as the definition of "credit reporting" in the context of the Fair Credit Reporting Act, or "financial institution" under the Gramm-Leach-Bliley Act of 1999, can determine whether any statute at all will apply to the use of personal data.

There is a further important dimension to privacy law in the United States, and it relates to federalism. In the USA, there is a dual federal–state system of lawmaking. Legislative power is shared between the federal government and the fifty states. In particular, state law has played a historically important leadership role in privacy law. This state role goes back to the common law tort of privacy, which has long been the province of state law and state courts (Solove and Schwartz 2009).

In the realm of statutory law, states have also made significant contributions to information privacy law. Perhaps the best recent examples of such innovations at the state level are data breach notification statutes

and data disposal laws (Schwartz and Janger 2007: 915). California enacted the first data breach notification law in 2002; forty-six other states have followed it. With the enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009, the federal government now has a limited data breach notification obligation in place for health care information covered by federal health privacy law.

Data disposal laws are another recent state innovation. Twenty-six states have enacted such statutes. These laws typically require a business to engage in proper destruction of files with personal information. Other innovative state approaches include laws that restrict the use of social security numbers, provide consumers who are victims of identity theft with the ability to place freezes on their credit reports, and require businesses to supply these victims with the relevant records of transactions associated with their stolen identity. Finally, some states are developing substantive requirements for data security. These set requirements for personal data handling. Massachusetts is regarded as having the most detailed as well as strictest such standards (National Conference of Legislators n.d.).

The continuing lack of omnibus legislation

Certain aspects of the structure of US information privacy law can best be understood through reference to American federalism. One classic distinction is between express preemption, where Congress has in explicit terms declared its intention to preclude state regulation in a given area and implied preemption, where Congress, through the structure or objectives of federal law, has impliedly precluded state regulation in the area. Preemption can also take the form of either field preemption or conflict preemption. Field preemption occurs when Congress intended to occupy an entire field of regulation. Conflict preemption takes place where Congress did not necessarily intend complete exclusion of state regulation in a given area, but to block it where a particular state law conflicts directly with federal law, or interferes with the accomplishment of federal objectives (Epstein and Greve 2007: 1–5).

As this chapter has noted, there is no omnibus federal law in the United States. Even were one enacted, it would not be likely to explicitly preempt all state sectoral privacy law. The result of such a statute would be regulatory chaos as several hundred, perhaps even thousands, of state laws would be invalidated as courts decided how to apply the

necessarily general provisions of a federal omnibus law to specific situations. Omnibus field preemption is also unlikely. Information privacy law necessarily regulates many contexts in which entities use personal information, and a single law is unlikely to substitute for all the statutes already in place. Moreover, the federal interest in the regulation of information privacy is not so compelling as to displace all state concerns and state laws on the subject. Its interest can be contrasted in this regard with more typical areas for field preemption, such as nuclear safety or alien registration (*Pac. Gas & Elec. Co.* v. *State Energy Res. Conservation & Dev. Comm'n* (1983); *Hines* v. *Davidowitz* (1941)).

Under conflict preemption, as noted above, federal law blocks any state statute that frustrates its ends. A federal omnibus privacy law might cap or otherwise shape damages for statutory violations. It might regulate other general privacy issues such as rights of action. The merits of such a law would likely be mixed. An omnibus statute with conflict preemption would likely limit future experimentation by sectoral laws at both the federal and state levels. It would also run the risk of ossification.

The example of the Privacy Act of 1974 is illustrative in this regard. The Privacy Act is a sectoral statute, of course, but one that is far-reaching for the American system. It regulates how federal agencies collect, use, and transfer personal information. Yet the Privacy Act's flaws have remained intact for decades, including its problematic definition of "system of records" and its restriction of its protection to citizens and permanent residents. The bipartisan Privacy Protection Study Commission pointed to these and other problems in the statute as early as 1977 (Privacy Protection Study Commission 1977: 491). More recently, the White House's White Paper on "big data" called for broadening the statute's protections to non-citizens (Executive Office of the President 2014: 51–3). Instead, inaction remains the norm and the Privacy Act still has not been amended to make this change.

An omnibus law for the United States would prove even more difficult to amend than the Privacy Act. It would raise complex issues across many dimensions. The legislative issue of deciding appropriate kinds of preemption alone would lead to a legislative logjam of colossal proportions. Where should states be allowed enforcement powers? Which existing state laws should be grandfathered and permitted continuing existence? Should new sectoral state laws be permitted? Should only stricter sectoral state laws be permitted?

At any rate, the current system of sectoral privacy law is firmly entrenched. An omnibus privacy statute does not appear to be on the

Congressional horizon. The current model is also one in which federal sector privacy statutes typically are based on conflict preemption and establish standards that states are permitted to exceed.

Conflict preemption in sectoral laws: floors not ceilings

The federal government's inaction regarding new sectoral privacy law has largely left the creation of new laws to regulate new problem areas to the states. An example of such federal inaction causing a regulatory opening at the state level is data breach notification. Where the federal government has acted in the past, it typically enacts privacy statutes that preempt state law. These federal laws generally block only state laws that conflict with their statutory objectives. At the same time, these federal laws also permit greater privacy protection. In other words, the federal law sets a protective floor and not a ceiling.

The exception to this general rule is the Fair Credit Reporting Act (FCRA) of 1970 (15 USC § 1681a[d]). Both in its original enactment and its important amendment through the Fair and Accurate Credit Transactions Act (FACTA) of 2003, FCRA is an outlier to privacy federalism. This statute, one of the earliest information privacy laws in the United States, regulates how "consumer reporting agencies" furnish "consumer reports." FCRA preempts state law relatively broadly and does so by reserving a large number of subjects for federal law. These include the pre-screening of consumer reports, procedures, and requirements relating to the duties of a person who takes any adverse action with respect to a consumer, and procedures and requirements regarding the information contained in consumer reports. These are examples of subject matter preemption; the federal law occupies the regulatory area.

In 2003 FACTA amended FCRA, not only through subject matter preemptions but also through narrower restrictions targeted to mandated behavior. As an example, FACTA requires consumer-reporting agencies to place fraud alerts on consumer credit files under certain circumstances. In so doing, it streamlines an area of industry procedures while, at the same time, permitting states to engage in further regulation regarding the larger subject area, which is identity theft. The approach of FCRA and FACTA, which is to favor federal preemption that limits stronger state protections, is, however, not typical of privacy preemption in the USA.

To illustrate the more typical approach, we can consider the Video Privacy Protection Act (VPPA) of 1988, the Cable Communications

Policy Act of 1984, the Gramm-Leach-Bliley Act (GLBA) of 1999, the Children's Online Privacy Protection Act of 1998 (COPPA), and the Health Insurance Portability and Accountability Act (HIPAA) of 1996. These laws all permit states to enact statutes that are more protective of privacy.

To begin with the VPPA, its core purpose is to restrict disclosure of video rental information. Regarding preemption, and as the VPPA states, it preempts "only the provisions of State or local law that requires disclosure prohibited" by the VPPA. In a similar fashion, the Cable Communications Policy Act permits a state franchising authority, a state, or a municipality to develop stronger privacy protections than found in this federal law (47 USC § 555[d][2]). These entities have traditionally played an important part in regulating cable companies, and the Cable Communications Policy Act recognizes this historic role. As another example, and one we will explore in more detail below, the GLBA states that its privacy protections "shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in any State ... except to the extent that [the state law] is inconsistent" with the GLBA (15 USC § 6807[a]). The GLBA adds that preemption will occur "only to the extent of the inconsistency." The GLBA explicitly provides that a state law is not inconsistent with it when the state law provides a safeguard to "any person" that "is greater than the protection" under the GLBA (15 USC § 6807[b]).

Finally, HIPAA, like GLBA, permits greater privacy protections but forbids inconsistent state laws. The most important regulation under HIPAA for preemption purposes is the Privacy Rule, as amended most recently in 2013 by the final omnibus HIPAA Rule. HIPAA's Subtitle F contains a general preemption of any "contrary" provision of state law followed by exemptions for public health and health regulatory reporting. It also permits the Secretary of the Department of Health and Human Services to grant exceptions for state laws that are "necessary" for certain enumerated purposes or relate to controlled substances. Finally, it provides a specific exception for state laws that are "more stringent" than the HIPAA standards.

These privacy statutes open up a world of interpretative possibilities. The key issue is whether a state law is more protective of privacy or inconsistent with the federal law. The line can prove difficult to locate and involves both the judiciary and regulators in a process of identifying why aspects of state statutes are either inconsistent with a federal privacy statute or more protective of privacy.

The GLBA offers an initial example of the necessary interpretative work. Courts have evaluated the issue of whether a state law provision is more protective of privacy than the GLBA or is inconsistent with it. One issue concerns the GLBA's provision that permits companies to share the information of their customers with affiliated entities without permission of the affected person (Janger and Schwartz 2002: 1226–7). In other words, customers of financial institutions are not given the ability under the GLBA to block the sharing of their information with affiliated entities. Courts have upheld state laws that require consumer permission, or an opt-in, before financial institutions may share information with affiliated entities. The GLBA also sets an opt-out before sharing of information with unaffiliated entities (Janger and Schwartz 2002: 1226–7). Vermont law requires an opt-in instead of an opt-out before a financial institution may share information with an unaffiliated entity (Vermont Admin. Code 4-3-42: 2). This law has also been upheld as more protective, but not inconsistent with the GLBA.

Regulators have also been involved in the necessary interpretive work. The GLBA grants the Federal Trade Commission (FTC) regulatory authority, and the agency has acted pursuant to it. In response to inquiries from four states, the FTC found that the state's financial privacy laws provided greater consumer protection than the GLBA and, therefore, were not preempted by it. These states were Connecticut, Illinois, North Dakota, and Vermont. In its opinion letters, the FTC found that compliance with the state financial privacy opt-in laws was possible without frustrating the purposes of the GLBA (Federal Trade Commission 2001). As a result, these laws are not inconsistent with the GLBA and are not preempted by it.

HIPAA has also seen a similarly strong role by a regulatory entity. The key entity is the Office for Civil Rights (OCR) of the Department of Health and Human Services. The most important regulation under HIPAA for preemption purposes is the Privacy Rule, as amended most recently in 2013 by the final omnibus HIPAA Rule. HIPAA's Subtitle F contains a general preemption of any "contrary" provision of state law followed by exemptions for public health and health regulatory reporting. It also permits the granting of exceptions for state laws that are "necessary" for certain enumerated purposes or relate to controlled substances. A further exception is provided for state laws that are "more stringent" than the HIPAA standards. There has been considerable litigation about the HIPAA Privacy Rules and whether a law is contrary to HIPAA or more stringent than it.

Different institutional actors

A large part of privacy preemption in the United States is shaped through institutional choices and behavior. Roderick Hills has argued that federalism is a matter of "how the federal and state governments interact, not in how they act in isolation from each other" (Hills 2007: 4). As these entities interact, the question of institutional design becomes a critical one. The GLBA and HIPAA grant the FTC and the Department of Health and Human Service's OCR, respectively, important roles in developing their respective statutory terms. Under the Cable Communications Policy Act, a state franchising authority, a state, or a municipality may develop stronger privacy protections than this federal law. Moreover, the judiciary, federal and state, is involved in deciding when state privacy law is inconsistent with a federal statute and when it is merely stricter.

The legislatures, federal and state, also play an important role in shaping preemption. By permitting preemption for stricter but not inconsistent laws, Congress has provided a roadmap for further state activity to promote privacy. As a more subtle way of promoting state legislative activity, Congress sometimes grandfathers in states with existing sectoral privacy legislation. For example, FACTA provides exceptions for some of its preemptive ceilings for California and Massachusetts (15 USC § 1681t[b][1][F]). These were the states that beat Congress to the regulatory punch and enacted state protections regarding identity theft before Congress took action through FACTA.

A final important institutional choice concerns enforcement of federal privacy law. Numerous federal privacy statutes permit enforcement by state attorney generals. These include the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act 2003, COPPA, FCRA, HIPAA, and the Telephone Consumer Protection Act 1991. One of the benefits of this approach is to reinforce the efforts of other federal enforcement agencies, such as the FTC. After all, the FTC includes privacy as only one of its many regulatory tasks, along with a role in antitrust, mergers, and consumer protection issues other than privacy. Moreover, state attorney generals are generally elected officials. Privacy is a popular issue, and one that is likely to be an attractive area for policy entrepreneurship, which is demonstrated by the COPPA actions brought by the state attorney generals in Texas and New Jersey, and the HIPAA actions of state attorney generals in Connecticut, Massachusetts, Minnesota, and Vermont.

The value of privacy federalism in a sectoral system

The United States features a dual system of federal and state sectoral regulations. This creates an opening for the states to experiment through legislation. Any of the fifty states can act first. This approach allows an opportunity for simultaneous experiments with different policies as well as consolidation of lessons learned.

Another benefit of privacy federalism is the decentralization of enforcement power. The Federal Trade Commission, the Department of Health and Human Services' OCR, state attorney generals, state and local cable franchise boards, and other entities all play a role in deciding when and how to enforce – and thereby develop – privacy laws. This decentralization allows decisions to be made at different levels of government and to reflect pluralistic policy concerns.

There is a final benefit of privacy federalism in the sectoral system of the USA. In the traditional model of federalism, a state law is followed by federal consolidation. The response to state action by a regulated entity is frequently to seek regulatory relief in Washington DC. This pressure for federal legislation can open opportunity for all policy stakeholders once the lawmaking process is open.

Today, however, there is considerable gridlock in Congress. Indeed, the current Congress is the least productive one since comprehensive statistics on federal legislative activity began to be kept in 1947. In short, the federal legislative process for privacy appears broken. It is a victim of the larger dysfunction in the Capitol.

In contrast, the state legislative process for privacy continues unabated. In 2013 the online newsletter of the International Association of Privacy Professionals spoke of a "tidal wave" of new privacy legislation from California (Finch 2013). That same year, *The New York Times* observed: "State legislatures around the country, facing growing public concern about the collection and trade of personal data, have rushed to propose a series of privacy laws" (Sengupta 2013). Legislation and legislative proposals continue unabated in 2014. In California alone, a dozen privacy bills were pending in June 2014 (State of California, Office of the Attorney General 2014).

Ideally, federal consolidation of state legislation provides benefits by avoiding inconsistent regulations, especially in areas with high cost and little positive results. Such a need currently exists for data breach notification legislation, where forty-seven different state statutes raise compliance costs for companies. The first such data breach notification statute,

that of California, was enacted in 2002, and the area is ripe for federal consolidation. For the White House, it is even a top priority (Executive Office of the President 2014: 51). Yet Congress does not appear to feel a sense of urgency concerning the enactment of such legislation.

There is a current absence of federal consolidation of state experimentation in privacy and security lawmaking. Regarding states-as-laboratories for policy innovations, Malcolm Feeley and Edward Rubin find such experiments "desirable, presumably ... not because of an abiding national commitment to pure research but because the variations may ultimately provide information about a range of alternative government policies and enable the nation to choose the most desirable one" (Feeley and Rubin 2008: 26). Congressional gridlock leaves the nation without consolidation of privacy experimentation. Statutory variations, such as in state data breach notification statutes, can increase compliance costs without adding commensurate policy benefits for individual privacy.

On a positive note, however, the social value of privacy federalism – its decentralization and development of pluralistic policy concerns – may have enduring power even in the age of gridlock and the absence of federal consolidation of state experimentation. In particular, information privacy norms do not exist a priori, but must be developed by individuals, social organizations, political entities, non-governmental organizations, and regulators. These entities define and elaborate a response, sometimes including regulations, to new kinds of technologies and social forms. Privacy federalism ensures diversity and competition in the resulting responses.

The diversity and competition in resulting state regulation will result from the different mix of intermediate interests, including citizen groups and lobbyists, with different kinds of power in various states. In contrast to other kinds of federalism battles in the United States, however, responses to privacy issues do not typically reflect a Democratic or Republican perspective and "flesh out nationwide controversies" at the state level (Bulman-Pozen 2014: 1946).

EU privacy federalism

As an initial matter, one can only speak of EU "federalism" on its own terms – it is not the equivalent of this legal concept in the United States. There are too many differences in the law and organization of the EU and USA for that to be possible. To single out an initial difference, one can point to the EU concept of "indirect administration." From the early

days of the European Community, this intergovernmental association has rested on "indirect administration," which means that the power to implement the law of the Community rests primarily with the member states. In the United States, however, federal power is expressed not only through legislation, but also the implementation of laws through the executive branch. We now consider how member states and EU institutions have shared regulatory power under the Data Protection Directive and then discuss the Draft Data Protection Regulation.

The Data Protection Directive and changes in the EU

The 1995 Data Protection Directive is a "harmonizing" instrument. This term means that it is not directly binding, but relies on member states to enact legislation that reflects its common rules for information privacy among EU member states. In the analysis of Spiros Simitis, the Directive is a "patchwork" that corrects and modifies elements of then existing national data protection law (Simitis 1997: 61–3).

Post-Directive, the focus of EU data protection law still remains at the level of the Member State. The Directive left the national lawmaker a "margin for maneuver," that is, to express national differences in their respective statutes. It also left national data protection authorities and courts with the responsibility of enforcing national legislation. The result has generally been viewed as unsatisfactory. Significant regulatory disparities exist among different nations' privacy law. As a result, international companies face twenty-eight different regulatory regimes when seeking to comply with EU privacy law. In summing up this sense of dissatisfaction, the Proposed Data Protection Regulation states: "Heavy criticism has been expressed regarding the current fragmentation of personal data protection in the Union, in particular by economic stakeholders who asked for increased legal certainty and harmonization of the rules on the protection of personal data" (European Commission 2012: 4).

At the same time, other events have shifted power in the EU away from the member states and to EU institutions. One of these milestones was the Lisbon Treaty of 2007,[1] which increases the role of the so-called "federal" institutions, the Commission, European Parliament, and Court of Justice. It also makes the Charter of Fundamental Rights binding on EU institutions and on member states when implementing EU

[1] O.J. [C 306], 2007. Accessed from http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:C:2007:306:TOC.

law. As a further matter, the Lisbon Treaty provides that the Union is to accede to the Charter of Fundamental Rights of the European Union (CFR). The CFR protects information privacy in its Article 8. In its Article 16(1), the Lisbon Treaty itself provides for a right to the protection of personal data.

Subsequent to the enactment of the Directive, EU courts have acted to protect privacy and to develop EU case law in this area. The European Court of Justice has issued important decisions concerning websites (*Lindqvist*, C-101/01 [Nov. 6, 2003]), the independence of data protection authorities (*Commission* v. *Germany*, C-518/07 [Mar. 9, 2010]), the European Data Retention Directive (*Ireland* v. *Parliament and Council*, C-301/06 [Feb. 10, 2009]), and, most recently, a "right to deletion" vis-à-vis search engines (*Google* v. *Gonzalez*, C-131/12 [May 13, 2014]). In June 2014, moreover, the High Court of Ireland issued an opinion asking the European Court of Justice to decide if the Irish data protection commissioner is "absolutely bound" by the EU's finding in 2000 that the Safe Harbor Agreement provides "adequate" data protection (*Maximillian Schrems* v. *Data Protection Comm'r* (2013)). High Court Judge Gerard Hogan wrote: "There is, perhaps, much to be said for the argument that the safe harbour regime has been overtaken by events" (*Maximillian Schrems* (2013): 32). The opinion cautiously added that the leaks about spying by Edward Snowden might be seen as exposing "gaping holes" in US data protection practices (*Maximillian Schrems* (2013): 32).

As for the European Court of Human Rights, it has ruled in numerous cases involving data protection (Press Unit 2014). These include cases concerning combatting terrorism (*Klaas and Others* v. *Germany* (1978)), the interception of correspondence of detained person (*Pisk-Piskowski* v. *Poland* (2005)), the electronic surveillance of communications (*Taylor-Sabori* v. *the United Kingdom* (2002)), the bugging of a residence (*P.G. and J.H.* v. *the United Kingdom* (2001)), the access to governmental databases about a person (*Brunet* v. *France* (2014)), rights in personal medical information (*Peruzzo and Martens* v. *Germany* (2013)), and the necessary safeguards for personal data in the employment context (*Copland* v. *the United Kingdom* (2007)). With reference to these opinions and the European data protection rights on which they rest, Kai von Lewinski has observed: "In data protection law, Europe no longer speaks German or French: it speaks European" (von Lewinski 2012: 217). This development of fundamental European rights to safeguard data protection helped set the stage for the Proposed Data Protection Regulation.

The road ahead: the proposed Data Protection Regulation

In January 2012 the EU released its Proposed General Data Protection Regulation. This document marks an important policy shift from directives to regulations. In EU law, as has been noted, a directive requires harmonizing legislation from the member states. In contrast, a regulation establishes directly enforceable standards. Christopher Kuner has explained the significance of this change: "a regulation leads to a greater degree of harmonization, since it immediately becomes part of a national legal system, without the need for adoption of separate national legislation; has legal effect independent of national law; and overrides contrary national law" (Kuner 2012: 217). In March 2014 the EU Parliament overwhelmingly voted to adopt the Regulation. The next stage will involve the Council agreeing on the text. Negotiations will then take place among the Parliament, the Council, and the Commission.

In the USA, the privacy community has focused on the Proposed Regulation's expression of individual rights. These protections begin by reaffirming the bedrock EU concept of forbidding any processing of personal information in the absence of a legal basis for the activity. The Proposed Regulation also strengthens existing requirements for data minimization; establishes privacy interests for children, defined as those under 13 years old, and creates an interest in portability of data. Beyond these safeguards, it develops a controversial "right to erasure" (COM 2012) and elaborates stricter requirements before consent can be used as a justification for data processing (COM 2012, Art. 7: 45). It also puts emphasis on the EU concept of protection from automated processing, which the Proposed Regulation combines with limitations on "profiling" (COM 2012, Art. 2: 40–41). It also restricts the use of sensitive data (COM 2012, Art. 43: 71–73).

Beyond these enhancements of privacy rights, the Proposed Regulation contains measures that destabilize the organizational status quo among the law and institutions of European privacy law. The result centralizes data protection decision-making in the Commission. As Niko Härting observes, the Draft Regulation placed the Commission at the top of the institutional pyramid for controlling data protection in Europe (Härting 2012: 460). The critical steps in this regard concern the Proposed Regulation's "consistency mechanism" (COM 2012, Art. 57: 82) and the power that it grants to the Commission to create a wide range of "delegated" and "implementing" acts (COM 2012, Art. 86: recital 37–38).

The first such action that shifts power to Brussels is the Proposed Regulation's "consistency mechanism." The Proposed Regulation creates a new institution, the European Data Protection Board (EDPB) (COM 2012, Arts. 64–72; Arts. 86–89). In so doing, it upgrades the status of the Article 29 Working Party, the panel of national supervisory authorities (COM 2012, Art. 64, 86). The EDPB provides a useful forum in which national supervisory authorities can reach a consensus about important issues. Governmental officials in individual countries with data protection legislation, in particular France, Germany, and the United Kingdom, played a central role throughout the 1980s and 1990s in the creation of supranational privacy protection in Europe (Newman 2008: 88–9). The EDPB offers a new institutional framework for drawing on these important ties. While the EDPB permits each national data protection commission to make final regulatory choices, it requires a draft proposal to be filed with it and the European Commission before a commission can adopt a measure relating to certain kinds of matters. The pre-filing requirement extends to matters affecting information processing in several member states, international data transfers, and a variety of other topics. The EDPB's subsequent recommendations will be valuable to the process of developing consensus about important transnational privacy issues among all member states. The EDPB would offer an opinion on the matter by simple majority.

More controversially, the Proposed Regulation grants significant new power to the Commission. It assigns the Commission the authority under the consistency process to issue opinions to "ensure correct and consistent application" of the Regulation. At an initial stage, the national data protection authority must "take utmost account of the Commission's opinion" (COM 2012, Art. 59[2]: 84). Additionally, the Commission may require national data protection authorities "to suspend the adoption" of a contested draft measure (COM 2012, Art. 60[1]: 84). Thus, through the consistency process, the Proposed Regulation grants the Commission the final word on a wide range of matters concerning the interpretation and application of the Proposed Regulation throughout the EU and beyond.

The Proposed Regulation also assigns the Commission the power to adopt "implementing acts" and "delegated acts" under a wide range of circumstances. Implementing acts enact procedures to put legislation into effect, and delegated acts supplement or amend nonessential elements of EU legislation. The Proposed Regulation contains numerous grants of power to adopt both kinds of acts, plus a general grant in Article 62(1) to issue implementing acts to decide "on the correct application" of

the Regulation under almost limitless circumstances (COM 2012, Art. 62[1]: 85). One analysis of the Proposed Regulation has found that it identifies forty-five different areas that can be regulated through such acts (Dix 2012: 321). As Kuner concludes, the result is "a substantial shifting of power regarding data protection policymaking from the EU member states and the [data protection authorities] to the Commission" (Kuner 2012: 227).

The EU's turn away from privacy federalism

There has been considerable controversy in Europe about the Proposed Data Protection Regulation. In Germany, the Bundesrat, or Federal Council, which represents the sixteen states of Germany in the federal legislative process, issued a resolution objecting to the Proposed Regulation (*Bundesrat Drucksachen*). It declared that the Proposed Regulation engages in an "almost complete displacement of the data protection rules in member states" (*Bundesrat Drucksachen* n.d.: 3). In France, the National Commission on Information Technology and Liberties (CNIL) objected to the regulation as "a centralization of the regulation of private life for the benefit of a limited number of authorities, and equally for the benefit of the Commission, which will gain an important normative power" (CNIL 2012). It also pointed to aspects of the Regulation that reinforce the "bureaucratic and distant image of community institutions" and reduce the status of data protection commissioners to that of a "mailbox" for passing on complaints to other authorities (CNIL 2012).

There has also been an outcry against the reliance in the Proposed Regulation on delegated and implementing acts. The resistance is demonstrated by leaked comments dated July 18, 2012 from member states to the Council of the EU (Note from Gen. Secretariat 2012). The national delegations of France, Germany, Italy, Luxembourg, Norway, Sweden, Poland, and the United Kingdom all objected to this aspect of the Proposed Regulation. As the objection from Poland noted, for example, the Proposed Regulation constituted a "rather general basis for the future shape of the future data protection system instead of coherent, seamless and in particular transparent regulation" (Note from Gen. Secretariat 2012: 101). One problem was that certain delegated acts were too broad, such as the authority of the European Commission to define "legitimate interests" of the data controller in specific data processing situations and in specific sectors.

Commentators have also wondered whether the Regulation violates "subsidiarity," a key tenet of EU law. Alexander Dix, the Berlin Data Protection Commissioner, argues that "the powers that the Commission grants itself in this process go far beyond the permissible" (2012: 321). A long-standing advocate of the "modernization" of EU data protection, Alexander Roßnagel finds the Proposed Regulation to represent the wrong kind of reform. He criticizes it as a "highly radical solution" that is based on a "centralized and monopolized regulation" (Roßnagel 2012: 553). Roßnagel calls for a "fully harmonized" Regulation "only where it was truly necessary for reasons of business competition" and a requirement in all other areas of merely a minimum standard with room for experimentation by member states (Roßnagel 2012: 555).

Relatedly, commentators have also found that the Proposed Regulation violates the EU principle of proportionality, which is a means-end test (Ronellenfitsch 2012: 562; Schild and Tinnefeld 2012: 316). Johannes Masing, a Justice of the German Federal Constitutional Court, has emerged as an important critic of the Regulation. In advocating for federalism and its benefits, he argues against the Proposed Regulation's high degree of centralization of power in European institutions. In his view, "the power of every federal structure lies in its diversity" (Masing 2012: 2310). He feels the lesson that the Proposed Regulation largely ignores is that a federal system benefits from an ability to draw on "a living laboratory for the discovery and testing of new sectoral and differentiated solutions" (Masing 2012: 2311).

Without a doubt, the Proposed Data Protection Regulation represents a decisive shift in institutional power – and one away from the member states. To be sure, the Proposed Data Protection Regulations reserves some matters for the member states. These include laws concerning national security, the media and freedom of opinion, health, "professional secrecy," telecommunications law, and church and religious associations law. Nonetheless, the Proposed Regulation occupies a large field and will make data protection overwhelmingly a matter of EU law.

In interpreting this new EU law of privacy, the final and most important judicial decision-makers will be the European Court of Justice and the European Court of Human Rights. National courts will still have a role in deciding issues of data protection law, but they will largely be interpreting and applying the Regulation rather than their respective national omnibus statutes. This development will curtail the development of national data protection traditions.

There will likely also be a lack of resources for the most important European courts with the responsibility for resolving important privacy matters. In the estimation of Masing, the European Court of Human Rights currently faces more than 170,000 pending cases to be decided by its 47 judges (Masing 2011: 10). More broadly, the development of national privacy traditions, linked to local concerns and traditions, has been a source of strength for European privacy law. In the past, the EU has acknowledged this need for relative discretion to be left to member states to interpret the European Convention on Human Rights based on factors such as their different histories and cultural backgrounds. An example of a resulting strong national tradition has been the German Federal Constitutional Court's development of its Basic Law, the post-war German constitution, to articulate first a right of informational self-determination (BVerfG Decision 65, 1, 43, 1983) and, more recently, a right to integrity and confidentiality in communication systems (BVerfG Decision 120, 274 Online-Searches, 2008).

The Regulation also enshrines the Commission as the critical decision-maker through the power given to issue delegated and implementing acts. As an initial example, a delegated act is to set out the circumstances in which notification of a data breach will be provided (Art. 32[5]). The experience with state data breach notification laws in the USA has shown that these issues, including the precise trigger for notification, are critical issues for which a wide range of policy choices are available. Moreover, another delegated act is to provide details regarding the balancing under Article 6(5) of the Regulation between the legitimate interests of the data controller and the interests or fundamental rights of data subject. A processing of personal data will only be permissible when the balance favors the data controller, which makes the elements of this balancing test one of the most important open issues under the Regulation.

In evaluating the impact of these delegating and implementing acts, one also confronts the likelihood of post-enactment difficulties for companies in the face of regulatory indeterminacy. In the period after enactment of the Regulation but before the Commission issues the most important delegated and implementing acts, there will be many open issues – and without national law to fill in the gaps. Here, too, questions of resources are likely to be paramount. In noting the large number of delegating and implementing acts, under the Regulation, Kuner (2012) has questioned the ability of the Commission to generate the delegated and implementing acts within any reasonable time frame. He writes: "the complexity

of the issues involved, together with political forces, likely will lead to a delay in adoption of many of them" (Kuner 2012: 14). Kuner notes that, according to one estimate, it may take *fifteen years* for all delegated and implemented acts to be enacted.

Thus the Proposed Regulation's break with privacy federalism raises, at a minimum, new risks. There are also steps that can be taken to protect federalism in EU privacy law. For example, Masing (2011) calls for development of a politically responsible Data Protection Commissioner, whom the Parliament would elect. This is a valuable proposal to help overcome any democratic deficit in EU data protection. The Proposed Regulation currently grants the Commission a problematic power over the national data protection authorities through the consistency process.

Finally, there is the impact of this power of the Commission on the larger democracy deficit in the EU. Here, Masing (2011) proposes creation of a new body, the EU Data Protection Authority. This new entity is to be located within the EU Parliament, which is the sole elected branch of the EU government. In this proposal, the EU Data Protection Authority would consist of representatives from the Parliament; the European Data Protection Board, which is the Proposed Regulation's forum of national data protection commissioners; and the already existing European Data Protection Supervisor, an independent EU office. This institution would further the establishment of checks and balances by dividing the ultimate power of the controversial new consistency process.

Other proposals are possible. For example, the EU might reduce the scope of the Proposed Regulation. The Proposed Regulation creates binding law for member states in a way that occupies too many areas, sweeps too broadly, and leaves too little room for future policy experiments. As a further matter, a revised regulation should respect subsidiarity by reducing the scope for implementing and delegated acts. Such acts should be limited to the topics of a more modest, revised regulation and concentrate on field definitions and the workings of the EU Data Protection Commission. This step will leave adequate room for further policy experiments at the national level.

This chapter has argued that privacy federalism in the United States helps to develop pluralistic policies. It safeguards diversity and competition in the responses and regulations to new technologies and social developments. This diversity and competition in regulation result from the differing mix of intermediate interests in the fifty states. The promise of privacy federalism is at once different and similar in the EU. The account of the positive value of privacy federalism in the United States did

not rest on separate state political identities. Indeed, there is no political culture on privacy issues that radically divides regions or states. Through the caldron of state identity, such as it may exist, California, New York, or Arkansas have not developed a strong sense of normative answers for privacy questions.

Here, privacy federalism may serve a different role in the EU, and one that cautions against too strong a suppression of national norms in favor of Brussels. In particular, there are (still) vivid national identities in European member states as well as political cultures that are strongly national in character. Moreover, and specific to this context, the weight of the past has shaped national responses to informational privacy questions in Europe. To pick only two examples, and at the risk of simplifying matters, the United Kingdom's data protection law reflects free speech concerns while Germany's law reflects its experience with oppressive native regimes on its own soil. These kinds of differences recommend at least some autonomy in the member states to develop different answers to the risks and challenges of personal information processing.

The similar promise of privacy federalism in the USA and EU alike concerns the general merit of diversity and competition in responses. As noted, a different mix of political power among constituents, legislatures, executives, and lobbyists will exist in the various fifty states in the USA. A similar landscape will exist in the member states of the EU. To the extent that the resulting divergent results and guarantee of "regulatory friction" for the regulated entities is seen as a benefit, privacy federalism guarantees a condition of ongoing joint regulation. At first view, at least, the Regulation seems to have gone too far in the other direction.

Conclusion

This chapter has drawn a contrast between the legal structures for information privacy in the USA and EU. The USA faces the risk of increasing fragmentation as individual states continue to enact privacy statutes and the federal lawmaker remains silent. There will be many regulatory "inputs" from the states with too little consolidation at the federal level. The EU faces a risk of too few future "inputs" from the member states and too much power consolidated at the Commission. In the USA, the challenge consists of revitalizing federal legislative involvement in the field of information privacy. In the EU, the goal should be creation of data protection law that is attentive to checks and balances in the Community. Here,

the Lisbon Treaty is illustrative. Jean-Claude Piris, the Legal Counsel of the Council of the EU, views the Lisbon Treaty as following in the tradition of "successive modifications of the founding Treaties" in demonstrating a decision "not to establish any single EU institution as politically too powerful" (Piris 2010: 237). Moreover, as Anne-Marie Slaughter points out, power in the transgovernmental realm should reflect "the guarantee of continual limitation of power through competition and overlapping jurisdiction" (Slaughter 2004: 259). The resulting balance of power should distribute privacy policymaking power among different EU and international institutions. The current Proposed Regulation falls short in this regard.

References

Bulman-Pozen, J. 2014. "From sovereignty and process to administration and politics," *Yale Law Journal* 123: 1920–56.

Bundesrat Drucksachen [BR] 52/1/12 (Germany).

COM 2012. *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), final*, January 25, 2012.

CNIL (Commission Nationale de l'informatique et des Libertés) 2012. *Projet de règlement européen: la défense de la vie privée s'éloigne du citoyen* [*Proposed European Regulation: Defense of Private Life Moves Away from Citizens*], January 26, 2012.

Dix, A. 2012. "Datenschutzaufsicht im Bundesstaat – ein Vorbild für Europa," [*Data Protection Oversight in the Federal State – A Model for Europe*] *Datenschutz und Datensicherheit* 36: 318–21.

Epstein, R. A. and Greve, M. S. 2007. "Introduction: Preemption in Context," in Epstein, R. A. and Greve, M. S. (eds.) *Federal Preemption: States' Powers, National Interests*. Washington DC: AEI Press, pp. 1–5.

European Commission 2012. *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*.

Executive Office of the President 2014. Big Data, Seizing Opportunities, Preserving Values. Washington DC.

Federal Trade Commission 2001. *North Dakota Privacy Law is Not Preempted*, 2001 WL 729771.

Feeley, M. M. and Rubin, E. 2008. *Federalism: Political Identity and Tragic Compromise*. University of Michigan Press.

Finch, K. 2013. "Straight From the Pacific Ocean: A Tidal Wave of California Privacy Laws," *The Privacy Advisor*, November 6, 2013.

Härting, N. 2012. "Starke Behörden, schwaches Recht –der neue EU-Datenschutzentwurf," [Strong Authorities, Weak Law – the new EU Data Protection Draft] *Betriebs-Berater* 8: 459–66.

Hills, R. M. Jr. 2007. "Against preemption," *New York University Law Review* 82: 1–68.

Janger, E. J. and Schwartz, P. M. 2002. "The Gramm-Leach-Bliley Act, information privacy, and the limits of default rules," *Minnesota Law Review* 86: 1219–61.

Kuner, C. 2012. "The European Commission's Proposed Data Protection Regulation: a Copernican revolution in European data protection law," *Privacy & Security Law Report* 11: 215–30.

Masing, J. 2011 "Ein Abschied von den Grundrechten," [A Farewell to Fundamental Rights] *Sueddeutsche Zeitung*, January 9, p. 10.

Masing, J. 2012. "Herausforderungen des Datenschutzes," [Challenges for Data Protection] *Neue Juristische Wochenschrift*: 2305–11.

National Conference of State Legislatures, n.d. *State Security Breach Notification Laws.*

Newman, A. L. 2008. *Protectors of Privacy.* Ithaca: Cornell University Press.

Note from Gen. Secretariat to Working Grp. on Info. Exch. & Data Prot. 2012. *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)* (July 18, 2012).

Piris, J.-C. 2010. *The Lisbon Treaty: A Legal and Political Analysis.* Cambridge University Press.

Press Unit, European Court of Human Rights 2014. *Factsheet: Data Protection* (September 2014).

Privacy Protection Study Commission 1977. *Personal Privacy in an Information Society.* Washington DC.

Roßnagel, A. 2012. "Editorial: Datenschutzgesetzgebung: Monopol oder Vielfalt?," [Data Protection Legislation: Monopoly or Diversity?] *Datenschutz und Datensicherheit* 36: 553–5.

Ronellenfitsch, M. 2012. "Fortentwicklung des Datenschutzes: Die Pläne der Europäischen Kommission," [Further Development of Data Protection: The Plans of the European Commission] *Datenschutz und Datensicherheit* 36: 561–3.

Schild, H.-H. and Tinnefeld, M.-T. 2012. "Datenschutz in der Union – gelungene oder missglückte Gesetzentwürfe?" [Data Protection in the Union: Successful or Unsuccessful Bill?] *Datenschutz und Datensicherheit* 36: 312–17.

Schwartz, P. M. and Janger, E. J. 2007. "Notification of data security breaches," *Michigan Law Review* 105: 913–84.

Sengupta, S. 2013. "No U.S. Action, So States Move on Privacy Law," *The New York Times*, October 30.

Simitis, S. 1997. "Einleitung in die EG-Datenschutzrichtlinie" in Dammann, U. and Simitis, S. (eds.) *EG Datenschutzrichtlinie – Kommentar.* Baden-Baden: Nomos.

Slaughter, A.-M. 2004. *A New World Order.* Princeton University Press.

Solove, D. J. and Hartzog, W. 2014. "The FTC And The New Common Law Of Privacy," *Columbia Law Review* 114: 583–676.

Solove, D. J. and Schwartz, P. M. (eds.) 2009. *Information Privacy Law*, Third Edition. New York: Aspen Publishers.

State of California, Office of the Attorney General 2014. *Privacy Legislation Pending in 2014.*

von Lewinski, K. 2012. "Europäisierung des Datenschutzrechts, Umsetzungsspielraum des deutschen Gesetzgebers und Entscheidungskompetenz des BVerfG," *Datenschutz und Datensicherheit* 8: 564–70.