New York University School of Law

The Jean Monnet Center for International and Regional Economic Law & Justice

THE NYU INSTITUTES ON THE PARK

Jean Monnet Working Paper Series

JMWP 18/15

Bilyana Petkova

THE SAFEGUARDS OF PRIVACY FEDERALISM

Cover: *Billy The Kid, 2000,* Steven Lewis

The Jean Monnet Center for International and Regional Economic Law & Justice

THE NYU INSTITUTES ON THE PARK

THE JEAN MONNET PROGRAM

J.H.H. Weiler, Director
Gráinne de Burca, Director

Jean Monnet Working Paper 18/15

Bilyana Petkova

THE SAFEGUARDS OF PRIVACY FEDERALISM

NYU School of Law • New York, NY 10011
The Jean Monnet Working Paper Series can be found at
www.JeanMonnetProgram.org

ISSN 2161-0320 (online)
Copy Editor: Danielle Leeds Kim

New York University School of Law
New York, NY 10011
USA

Publications in the Series should be cited as:
AUTHOR, TITLE, JEAN MONNET WORKING PAPER NO./YEAR [URL]

THE SAFEGUARDS OF PRIVACY FEDERALISM

BILYANA PETKOVA*

ABSTRACT

The conventional wisdom is that neither federal oversight nor fragmentation can save data privacy any more. I argue that in fact federalism promotes privacy protections in the long run. Three arguments support my claim. First, in the data privacy domain, frontrunner states in federated systems promote races to the top but not to the bottom. Second, decentralization provides regulatory backstops that the federal lawmaker can capitalize on. Finally, some of the higher standards adopted in some of the states can, and in certain cases already do, convince major interstate industry players to embed data privacy regulation in their business models.

* Postdoctoral Fellow-in-Residence at New York University School of Law AY2014/15 and Visiting Fellow at Yale Information Society Project. Contact e-mail: bilyana.petkova@yale.edu; bilyana.petkova@eui.eu

This paper is forthcoming in the Lewis & Clark Law Review, Vol.20, Issue 2

I am indebted to Heather Gerken, Chris Hoofnagle, Roderick Hills, Jason Schultz, Ira Rubenstein, Helen Nissenbaum and Nate Wessler for their valuable feedback, as well as to the NYU Jean Monnet Center and the Yale Information Society Project for making this research possible. I owe special thanks to Robert Post, Jack Balkin, Paul Schwartz, Gráinne de Búrca and Jules Polonetski for the overall support. The organizers and participants in the 8th Annual Privacy Law Scholars Conference held at Berkeley on 4-5 June 2015 and the "Surveillance, Privacy and Transnational Relations in the Digital Era" conference held in Brussels on 12-13 March 2015, as well as the NYU Privacy Research Group provided great comments and suggestions for this article and my future research. The usual disclaimer applies.

INTRODUCTION: US PRIVACY LAW STILL AT A CROSSROADS

It is hardly surprising that in the wake of rapid technological developments on the one hand and a constant push toward a "surveillance state" on the other, data privacy law is in flux in the United States. It is surprising, however, how little the debate has progressed over the years. As noted by Professor Hoofnagle,[1] the conversation on data privacy has changed strikingly little since the 1973 landmark report of the US Department of Health, Education, and Welfare (HEW) published the Fair Information Practice Principles (FIPPs) that were to become the backbone of privacy laws worldwide. Yet, the United States – where as far back as 1890 Warren and Brandeis proclaimed a "right to be left alone"[2] and where the FIPPs originated in the influential HEW report[3] – has hesitated to take a decisive stance on data privacy since then.[4] In providing legal certainty, a level of consolidation of data privacy laws can be beneficial to individuals, businesses and law enforcement alike, but how to arrive at the right level of regulation? The value of privacy

[1] Chris J. Hoofnagle, *The Origin of Fair Information Practices: Archive of the Meetings of the Secretary's Advisory Committee on Automated Personal Data Systems (SACAPDS)*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2466418 (2014); Paul M. Schwartz, *The EU-US Privacy Collision: A Turn to Institutions and Procedures* 126 HARV. L. REV. 1966, 1969-1970 (2013) (discussing early concurrent developments on both sides of the Atlantic, the importance played by the United States in information privacy debates worldwide at that early stage and initial convergence in the US, European countries and on the supranational level that by the 1980s led to a "...consensus that information privacy statutes were to be constructed around Fair Information Practices..."); Robert Gellman, *Fair Information Practices: A Basic History*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020&download=yes (referring to a 1972 study in Great Britain that focused on private organizations' threat to privacy and like the HEW report, revolved around a version of fair information principles). Cf. also Oliver Diggelmann and Maria Nicole Cleis, *How the Right to Privacy Became a Human Right* HUM. RTS. L. REV. (2014) (arguing that international agreements after World War II preceded the incorporation of the right to privacy in national constitutions around the globe).

[2] Samuel Warren and Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[3] The HEW report resulted in no small measure from the creative work and leadership of Willis Ware from the Rand Corporation of California, *see, e.g.* Robert Gellman, *Willis Ware's Lasting Contribution to Privacy: Fair Information Practices* 12 IEEE SECURITY & PRIVACY 51 (2014).

[4] This is all the more puzzling since the US Fair Credit Reporting Act (FCRA) anticipated the FIPPs already in 1970 and was one of the first statutory attempts to regulate the use of personal information by private entities worldwide, *see infra* note 20 pointing to the FCRA's later amendments. For an overview of consumer reporting in the US, *see* CHRIS J. HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (forthcoming, Cambridge Univ. Press, 2015). The primary problem with the FCRA might be enforcement "...[as] summarizing the elements of the FCRA make[s] clear, the consumer reporting industry never embraced the various privacy and fairness mandates imposed by Congress...Things may change now, however, as the CFPB [Consumer Financial Protection Bureau] can supervise and examine companies for compliance with the FCRA. This is likely to be more effective than enforcement actions, because the [Federal Trade Commission] FTC does not bring cases over minor compliance matters", *id*.

is constantly debated,[5] as is the legal framework within which to protect it. Should the US courts pronounce an autonomous right to informational privacy, as they once did about decisional privacy?[6] If so, should a right to privacy be designed to protect sensitive data and minority rights[7] only or does instead the sensitivity of the data depend on its use?[8] Or, perhaps, might the Fourth Amendment be stretched to cover a broader scope,[9] or in cases of automated decision-making – should (technological) due process kick in?[10] Alternatively, should privacy advocates look into resuscitating tort law or giving a broader purchase to the notion of confidentiality,[11] or should they place their bets on privacy as a property right?[12] Ultimately, can consumer privacy be realized through co-regulation between the public and the private sector[13] or left to the gradual development of a common law approach, which some claim is emerging through settlements enforced by the Federal Trade Commission (FTC)?[14] Many worthy ideas have been put on the table but thus far none have gained sufficient traction among US policy makers and other interested parties.[15]

---

[5] For a springboard of accounts going beyond the mainstream understanding of privacy as an individual value, cf. Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L REV. 957. Cf. HELEN NISSENBAUM, PRIVACY IN CONTEXT (2010) (theorizing the deficits of the privacy-as-control paradigm and offering to address these through contextualized norms).

[6] Griswold v. Connecticut, 318 U.S. 479 (1965).

[7] Scott Skinner-Thompson, *Outing Privacy*, Nw. U. L. Rev. (forthcoming 2015).

[8] Susan Landau, *Control the Use of Data to Protect Privacy*, 347 SCIENCE, 504 (2015); Craig Mundie (2014), *Privacy Pragmatism*, FOREIGN AFFAIRS, March/April 2014.

[9] Kevin Bankston & Margot E. Kaminski, *A Unified Reasonable Expectation of Privacy? What U.S. v. Jones Could Mean for Other Privacy Laws* (paper presented at the 8th Privacy Law Scholars Conference, June 2015, on file with author).

[10] Danielle K. Citron & Frank A. Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014); Jason Schultz & Kate Crawford, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. Rev. 93 (2014).

[11] Jack Balkin, *Information Fiduciaries and the First Amendment* (forthcoming 2015).

[12] Paul M. Schwartz, *Property, Privacy and Personal Data*, 7 HARV. L. REV. 2055 (2004); Lauren H. Scholz, *Privacy as Quasi-Property*, 7 IOWA. L. REV. (forthcoming 2015).

[13] Ira Rubunstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 I/S: J.L. & POL'Y FOR INFO. SOC'Y 356 (2011).

[14] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, COLUM. L.R. 583 (2014).

[15] One example is the failure (thus far) of the Obama administration to establish baseline protection for consumer privacy in 2012 and in 2015. *See* e.g. for the later version of the White House proposal: Consumer Privacy Bill of Rights Act of 2015, https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

At the same time, while EU is not a fully-fledged federation, in the area of data privacy it has opted for a high level of harmonization.[16] Historically, Germany was the first nation to adopt a data protection statute – first, on the local level – in the state of Hessen in 1970, and then as federal German legislation.[17] A few other European states followed suit, and by the time the (General) European Data Protection Directive of 1995 and the overall EU data protection framework were established, privacy was increasingly understood across the EU as a fundamental right[18] that protects self-determination and which must be balanced through proportionality with other rights and interests.[19] By way of comparison, current US privacy law is mostly composed of federal sector-specific statutes that offer variegated protection in the public and private sector with regard to different types of data.[20] Despite the differences between Europe and the United States, however, this article demonstrates that often one state, in this case, – California – is a frontrunner, while other states and the private sector gradually follow suit.

---

[16] European Parliament and Council Directive 95/46/EC, OJ L281/23 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Directive) and European Parliament and Council Directive 2002/58/EC, OJ L201/37 concerning the processing of personal data and the protection of privacy in the electronic communications sector (the e-Privacy Directive).

[17] "The Hessian Parliament's nearly unanimous and astonishingly quick enactment of the Data Protection Act was due, in part, to the limited scope of the Act – it addressed only the public sector's automated processing of personal data...Thus, the German Federal Data Protection Law was passed only after five years of intense controversies shaped by the requests to mitigate the duties of private data processors," Spiros Simitis, *Privacy – An Endless Debate*, 98 Cal. L Rev. 1989, 1996 (2010).

[18] Privacy is conceptualized as a fundamental right, enshrined in the constitutions and statutes of many of the EU Member States, as well as in the Charter of Fundamental Rights of the European Union art. 7, Oct. 26, 2012, O.J. (C 326), 391 [hereinafter EU Charter] and the European Convention of Human Rights, art. 8, Nov. 4, 1950, 213 U.N.T.S. 222. Moreover, alongside the established right to privacy, the EU Charter includes a separate right to data protection in art. 8.

[19] Worth mentioning is the German Federal Constitutional Court's judgment in the *Microcensus* case of 1969, which set up a framework allowing proportionality balancing. For an English excerpt *see* DONALD P. KOMMNERS & RUSSELL A. MILLER, THE CONSTITUTIONAL JURISPRUDENCE OF THE FEDERAL REPUBLIC OF GERMANY (2012). The proportionality test, similar to *strict scrutiny* in the US, would become the relevant framework within which the European Court of Justice (ECJ) and the European Court of Human Rights (ECtHR) adjudicate on privacy protection.

[20] Examples include the Health Insurance Portability and Accountability Act Regulations (HIPAA), 45 C.F.R. pt. 164 (2012); the Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2006), as amended by Video Privacy Protection Amendments Act of 2012, Pub. L. No. 112-258, 126 Stat. 2414 (2013); the Fair Credit Reporting Act 15 U.S.C. §§ 1681–1681x (2006 & Supp. V 2011); as well as the Family Educational Rights and Privacy Act of 1974 (FERPA), 20 U.S.C. § 1232g (2006 & Supp. V 2011) and the Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501 et. seq., partially amended with Health Information Technology for Economic and Clinical Health Act (HITECH) 42 U.S.C.A. § 17902 (2009); The Gramm–Leach–Bliley Act (GLBA), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended at 15 U.S.C. § 6803 (2012)).

Overall, the federated nature of lawmaking in both the US and the EU is seen to deliver sub-optimal results.[21] In particular, in the US there are concerns regarding the increased fragmentation of American data privacy law and the lack of relevant federal consolidation, whereas in the EU the proposed General Data Protection Regulation and currently debated anti-terrorism measures have generated opposition regarding the over-centralization of powers in European institutions.[22] The aim of this article is not to evaluate the various legal and policy proposals on their merits, but rather the more modest goal of challenging a commonly held assumption that obstructs lawmaking in this area. Even the most fervent data privacy advocates in the US can be wary of centralizing data privacy solutions for fear of regulatory "ossification" that would stymie innovation.[23] Even the most fervent opponents of intrusive surveillance methods temper their zeal for fear of tilting the balance too far on one side.[24] The underlying assumption seems to be that privacy regulation would be too "sticky" and impossible to undo or modify in correspondence with present-day technologies or security threats.

Recognizing that path-dependence factors in any choice of regulation, I provide evidence for the dynamism of privacy law through federalism: as federalism studies show, independent state institutions are challenging the *status quo* of privacy policies both in the US and in the EU, thereby contributing to a well-functioning democracy. The national parliaments, data protection authorities, and constitutional courts of EU countries, but also, increasingly, the state legislatures, attorneys general, and the highest state courts in the US provide substantive input to privacy law making. Ultimately, I argue that the centralization of privacy policies does not carry with it the risk of ossification, as long as

[21] Paul Schwartz, *The Value of Privacy Federalism*, *in* SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES, Beate Roessler & Dorota Mokrosinska, eds. (forthcoming 2015).

[22] Johannes Masing, Roßnagel, *Herausforderungen des Datenschutzes* [Challenges for Data Protection], NEUE JURISTISCHE WOCHENSCHRIFT 2305-11 (2012).

[23] Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 928 (2009) (outlining the dangers of omnibus regulation for the US).

[24] The recent difficulties surrounding the reform of the National Security Agency (N.S.A.) surveillance practices even in the wake of public outcry after the Snowden revelations and despite the firm stance subsequently taken by the US Court of Appeals for the Second Circuit, provide a ready example. *See* e.g. Charlie Savage, *Surveillance Court Rules that N.S.A. can resume Bulk Data Collection*, N.Y. TIMES, June 30, 2015, *available at*: http://www.nytimes.com/2015/07/01/us/politics/fisa-surveillance-court-rules-nsa-can-resume-bulk-data-collection.html?smid=nytcore-ipad-share&smprod=nytcore-ipad&_r=0.

the "democratic churn"[25] created by independent state institutions and put into practice in state regulation is entrusted to prompt the US national or the EU-wide system to change. What is more, technology increases the potential for "races to the top" in data privacy regulation both across state jurisdictions and in the private sector. Unlike in other fields where competitive federalism might also provoke "races to the bottom,"[26] the data privacy field presents a more or less clear-cut choice between effective regulation and non-regulation. Yet options for leveling up privacy protections get overlooked in what has become known as "the privacy thicket." The opportunity structures for "races to the top" need to be carefully studied by the relevant decision maker (e.g., the FTC, the US Congress, or the European institutions) that can capitalize on such trends to enhance privacy protection without excessive costs for businesses and law enforcement. Therefore, in an attempt to go beyond the binary divides,[27] I compare the US and the EU privacy systems in a vertical fashion, focusing on how little-theorized structural incentives[28] play a role in the development of privacy law in each of the two respective legal orders. In this sense, the article's goal is not to directly compare the two regimes' compatibility[29] but rather to provide insights on privacy law formation in each of the two federated contexts. By arguing for federal data privacy consolidation modeled after the states, I do not mean

[25] Heather K. Gerken, *Federalism All the Way Down*, 124 HARV. L. REV. 4, (2010) (disaggregating federalism down to actors on the local level).

[26] William L. Cary, *Federalism and Corporate Law: Reflections Upon Delaware* 83 Yale L. J. 663 (1974) ("Delaware is both the sponsor and the victim of a system contributing to the deterioration of corporation standards. This unhappy state of affairs, stemming in great part from the movement toward the least common denominator, Delaware, seems to be developing on both the legislative and judicial fronts...Perhaps now is the time to reconsider the federal role). Richard L. Revesz, *Rehabilitating Interstate Competition: Rethinking the "Race-to-the-Bottom" Rationale for Federal Environmental Regulation*, 67 N.Y.U. L. REV. 1210, 1210 (1992) (distinguishing the environmental from the corporate-charter and bank-charter literatures and pointing out that even if races to the bottom indeed existed in the environmental field, a federal response could not be the answer to such problems); Kirsten H. Engel, *State Environmental Standard-Setting: Is There a "Race" and Is It "To the Bottom"*?, 48 HASTINGS L.J. 271, 274 (1997) (arguing in rebuttal to Revesz that the interstate market for industrial development and environmental benefits is substantially distorted, and that a federal framework is needed to avoid social welfare loss).

[27] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1154 (2004).

[28] Paul M. Schwartz & Edward J. Janger, Notification of Data Security Breaches, 105 MICH. L. REV. 913, 925-932 (2007) (discussing regulatory, economic and reputational incentives on businesses to deal with data breaches).

[29] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy in Europe: Initial Data on Governance Choices and Corporate Practices*, 81 GEO. WASH. L. REV. 1529, (2013); *New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry*, 33 LAW & POL'Y 477 (2011)(presenting empirical evidence as to why privacy law on the ground (as opposed to on the books) in the US and the EU is converging more than acknowledged).

to suggest that the US should necessarily follow the EU model of omnibus regulation. Instead, privacy consolidation in the US can take place by extending the standards of protection applicable in one sector to another, by introducing new sectoral federal legislation, or through a Privacy Restatement that draws on state law, among other things, as a source.[30] Equally, I do not mean to suggest that Europeanizing data protection laws presents an ideal-type of privacy consolidation. Instead, I explore some of the in-built institutional mechanisms at the disposal of both the US and the EU to help safeguard the two systems from over-centralizing.

Part I summarizes the US and EU scholarly and policy debate on data privacy. Part II suggests a federalist theoretical lens, applicable to US and the EU privacy contexts alike. Looking at privacy as a case study of federalism helps dissipate the assumption of federal or European privacy regulation being too inflexible or burdensome to businesses. Part III presents empirical evidence for the role of state institutions in the US and the EU and state regulatory models as catalysts in federated privacy lawmaking. The empirical material is complemented by several semi-structured interviews with representative US interstate businesses, civil rights organizations, and governmental officials conducted in 2015. Part IV offers tentative conclusions about the intersection of privacy and federalism.

I. WHAT PRIVACY CAN LEARN FROM FEDERALISM AND FEDERALISM FROM PRIVACY

A condition *sine qua non* for states to function as "vital cells... of democratic sentiment, impulse and action"[31] is some degree of state autonomy. Both the US and EU governments are of limited powers but both are also deeply interconnected systems. State autonomy can thus be understood as preserving meaningful state regulatory responsibilities in a densely intertwined interstate web of federal and quasi-federal

[30] PRINCIPLES OF THE LAW, DATA PRIVACY, AMERICAN LAW INSTITUTE, ongoing project, http://www.ali.org/index.cfm?fuseaction=projects.members&projectid=30#MCG.

[31] Edward S. Corwin, *The Passing of Dual Federalism*, 36 VA. L. REV. 1, 2 (1950). *See also* Jessica Bulman-Pozen, *From Sovereignty and Process to Administration and Politics: The Afterlife of American Federalism*, 123 YALE L.J. 1626, 1154 (2014) (arguing that the US states lack an autonomous realm of action but infuse federal law with diversity and competition through party federalism).

constructs. In contrast to the allure of sovereignty and the resultant "double spheres" approach[32] that likely generates a more manageable judicial doctrine but is long outdated and outpaced by present-day realities, [33] state autonomy is a malleable concept. It inevitably invites questions of what exactly constitutes valuable self-government or meaningful regulatory responsibilities. To be sure, scholars of US federalism might reject or accept the anti-commandeering string of case law of the Supreme Court,[34] and see the "power of the servant" as either a form of autonomy gain[35] or an autonomy loss thereof.[36] In contrast, "commandeering," constitutes the bread and butter of everyday EU law functioning, but (but perhaps due to the different structure of the Union) has never been questioned as a serious threat to Member States' autonomy.[37] A prominent school of thought in the US locates state autonomy as lying outside the courtroom, preserved through the political process, primarily via states' representatives in the Senate.[38] With the consolidation of federal power, however, the political process has come to be

[32] Ernest A. Young, *The Rehnquist Court's Two Federalisms*, 83 TEXAS L. REV. 1-165 (2004). Young's rejection of the "doubles spheres" understanding holds well both for the US and the EU. For the European context, *see* ROBERT SCHÜTZE, FROM DUAL TO COOPERATIVE FEDERALISM: THE CHANGING STRUCTURE OF EUROPEAN LAW (Oxford Univ. Press, 2009). Young's conceptualization of sovereignty however appears too narrow since he understands state sovereignty to be limited to state immunity. *But see* the European context where Member States can be found liable for failure to implement EU law, Case C-6/90 and C-6/90, Andrea Francovich and Danila Bonifaci and others v. Italian Republic, 1991 E.C.R. I-05357.

[33] Heather Gerken, *Slipping the Bonds of Federalism*, 128 HARV. L. REV. 85, 99-101 (2014).

[34] *Compare* Ernest A. Young, *see supra* note 33 (accepting anti-commandeering as an expression of state autonomy), and Roderick M. Hills, Jr., *The Political Economy of Cooperative Federalism: Why State Autonomy Makes Sense and "Dual Sovereignty" Doesn't*, 96 MICH. L. REV. 813 (1998) (distinguishing the doctrine' rationale from protection of state sovereignty), with the New, New Federalists, *see supra* note 32 (rejecting anti-commandeering as a "bad theory that makes for not-so-bad case-law"), and Neil Siegel, *Commandeering and its Alternatives: A Federalism Perspective*, 59 VAND. L. REV. 1630 (questioning, among others, the Supreme Court's fixation on accountability as a justification for anti-commandeering).

[35] Heather K. Gerken, *Of Sovereigns and Servants*, 115 YALE L. J. 2633 (2006) (discussing the leverage gained by state administrators over the federal government in the oversight and implementation of federal programs)

[36] Richard A. Epstein & Mario Loyola, *The United State of America*, THE ATLANTIC, JULY 31, 2014 (mourning over the federal takeover of the states that started during the New Deal and intensified with the Affordable Care Act).

[37] The Member States implement EU statutes, be they directives or regulations. Under EU law, a regulation is directly applicable, i.e., it does not need to be transposed by a national legislative act into the domestic legal order, whereas a directive is binding as to its effect but leaves the choice of means to the Member State. In principle the Member States retain more leeway when implementing directives. *See* Daniel Halberstam, *Comparative Federalism and the Issue of Commandeering*, *in* THE FEDERAL VISION: LEGITIMACY AND LEVELS OF GOVERNANCE IN THE UNITED STATES AND THE EUROPEAN UNION 213, 231(Kalypso Nicolaidis & Robert Howse, eds., Oxford Univ. Press 2001).

[38] Herbert Wechsler, *The Political Safeguards of Federalism: The Role of the States in the Composition and Selection of the National Government*, 54 COLUM. L. REV. 543 (1954); Larry Kramer, *Putting the Politics Back into the Political Safeguards of Federalism*, 100 COLUM. L. REV. 215 (2000).

uniformly criticized as an inadequate safeguard of federalism.[39] As for the EU,[40] though the political safeguards are far stronger there,[41] the incremental consolidation of EU competences in a number of areas through the case law of the European Court of Justice (ECJ) and subsequent Treaty amendments have given rise to debates on "competence creep"[42] and fears of the continuous transfer of policies to the hands of unaccountable bureaucrats in Brussels. Like the Supreme Court before the "federalist revolution" of the Rehnquist bench, the ECJ is generally seen as an unreliable protector of Member States competence, often applying a double standard of review that is stringent toward the Member States but lenient toward the Union.[43] The adoption of a EU legally binding charter of fundamental rights and its contested scope of applicability to the Member States has recently fueled this debate. However, in an attempt to protect state interests, the EU has amended the founding Treaties to introduce mechanisms such as a subsidiarity check on EU legislation and a provision on protecting national constitutional identities.[44]

Fortunately in the US most federalism scholars concur in their opposition to preemption as a necessary precondition for state autonomy.[45] The "new federalism" of the 1980s and 1990s brought this debate into sharp focus as US state legislatures began

---

[39] The conclusions drawn from such criticisms, however, are diametrically different. *Compare* John C. Yoo, *The Judicial Safeguards of Federalism*, 70 S. CAL. L. REV. 1311 (1996) (arguing that the Court should step in to defend state sovereignty), with the New, New Federalists, *see Federalism as the New Nationalism: A dialogue among a new school of federalism scholars*, 123 YALE L.J. symposium issue (arguing that the states continue to play an important role, albeit trough other means, in the US federal system and rejecting calls for aggressive judicial review in federalism cases).

[40] Marc Tushnet, *How (and How Not) to Use Comparative Constitutional Law in Basic Constitutional Law Courses*, 49 ST. LOUIS U. L. J. 671, 677 (2005).

[41] Even too strong, as suggested by the dominance of national interests in the European Council revealed during the recent Greek debt crisis. *See* Tomas Dumbrovsky, *Europeanizing the Eurozone,* INT'L J. CONST. L. BLOG, July 31, 2015, *at: http://www.iconnectblog.com/2015/07/europeanizingtheeurozone.*

[42] *See* Paolo Carozza, *The EU Charter of Fundamental Rights and the Member States, in* THE EU CHARTER OF FUNDAMENTAL RIGHTS: POLITICS, LAW AND POLICY (Steve Peers and Angela Ward, eds., Hart Publishing, Oxford 2004); Sasha Prechal, *Competence Creep and General Principles of Law*, REV. EUR. ADMIN. L. (2010).

[43] Jason Coppel and Aidan O'Neill, *The European Court of Justice: Taking Rights Seriously?* 12 LEGAL STUD. 227 (1992).

[44] Article 4(2) reads: "The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State," Consolidated Version of the Treaty on European Union and the Treaty on the Functioning of the European Union, Sep. 26, 2012, O.J. (C 326) [hereinafter TEU and TFEU].

[45] *See supra* notes 34.

enacting laws that, in many areas, went beyond the federal floor of protection, and as state courts began reaching more rights-protective results than the Supreme Court when interpreting analog rights provisions under their own constitutions.[46] However, in the EU, under the ECJ's current interpretation of the EU Charter of Fundamental Rights,[47] the primacy and effectiveness of EU law is considered in almost absolute terms. Rejecting this monolithic understanding, EU law scholars have started making the case that even in areas under the scope of EU law the Member States can and should be given a certain leeway to espouse higher rights protection under their constitutions.[48] Similarly, scholars have advocated against judicial application of the Dormant Commerce Clause or statutory preemption in the US, as new state statutes eventually force controversial policy issues on the agenda of the federal (and by extension, it can be theorized – the European) lawmaker.[49] This may well be favorable to the democratic process: individuals and the states both benefit since, on the one hand, what can be politically thorny problems like air pollution, workplace safety, student privacy or the balance between privacy and security will have to be addressed despite Congress or the EU institutions dragging their feet. On the other hand, a federal (or EU level approach) can avoid externalization of costs by some states and "races to the bottom" by others, [50] if any. And, the industry will be able to

[46] G. Alan Tarr, *New Judicial Federalism in Perspective*, 72 NOTRE DAME L. REV. 1097 (1997).

[47] The text of the EU Charter certainly gives the possibility for reliance on more rights-protective sources. Article 53 reads: "Nothing in this Charter shall be interpreted as restricting or adversely affecting human rights and fundamental freedoms as recognized, in their respective fields of application, by Union law and international law and by international agreements to which the Union, the Community or all the Member States are party, including the European Convention for the Protection of Human Rights and Fundamental Freedoms, and by the Member States' constitutions", Charter of Fundamental Rights of the European Union, Sep. 26, 2012, O.J. (C 326) [hereinafter EU Charter].

[48] Whereas the Spanish Constitutional Court interpreted the EU Charter as a floor of protection to the right of fair trial in *Melloni*, the ECJ insisted on an absolute understanding of EU primacy. So the fact that state courts may still be able to enforce more protective constitutional rights in situations not entirely determined by EU law under *Melloni* might be little consolation for rights enthusiasts. And yet, as it is argued, "if the [ECJ] has admitted restrictions on [EU] primacy and effectiveness on the basis of more protective constitutional rights when the states derogate from the EU fundamental freedoms of movement [as in the *Omega* case], why not when the states implement secondary legislation?".... Even if the primacy, unity, and effectiveness of EU law are compromised, domestic constitutional rights should not be automatically set aside, but rather the [ECJ] should examine whether a restriction on those principles might be justified in order to accommodate more protective constitutional rights...", *Melloni in Three Acts: From Dialogue to Monologue*, 10 Eur. Con. L. Rev. 308, 328 (2014).

[49] Roderick M. Hills, Jr. *Against Preemption: How Federalism Can Improve the National Legislative Process*, 82 N.Y.U. L. REV. 1 (2007) (advocating against statutory preemption of state tort law) and Heather K. Gerken & Ari Holtzblatt, *The Political Safeguards of Horizontal Federalism*, MICH. L. REV. (2014) (arguing the benefits of state law spillovers against evoking the Dormant Commerce Clause).

[50] Jonathan R. Macey, *Federal Deference to Local Regulators and the Economic Theory of Regulation*, 75 VIRGINIA L. REV. 265 (1991).

reduce costs by working with one instead of multiple standards. The US Supreme Court has mainly attacked preemption on grounds of "states' police powers."[51] Yet this approach might lead autonomy to be associated with fistfights of state and federal zero-sum games, the result being that the very concept of autonomy collapses into sovereignty or a "double spheres approach" albeit with a softer edge.[52] Therefore, there seems to be no ready-made solution to the dilemma both the ECJ and the Supreme Court face in want of a doctrine that preserves space for the states while reflecting the intertwined nature of federal and state interactions.

In data privacy in particular, federalism's potential to generate regulatory experimentation is especially valuable to ensure a well-functioning and democratic system in both the US and the EU. The states can provide the celebrated "laboratories of democracy"[53] effect that is needed in the search for innovative regulatory solutions to balance privacy with countervailing interests. Moreover, in both the US and the EU time is of the essence. Whereas the checks and balances of US federal lawmaking could be understood as originally designed to guard the states from federal overreach,[54] at present the acute gridlock in Congress raises serious concerns on both sides of the political spectrum. Similarly, European lawmaking is a protracted process – in the case of the General Data Protection Regulation currently tabled for adoption, for example, three and a half years have passed since the lawmaking procedure was initiated and as of this writing, there has been still no final vote. In the face of rapid technological developments on the one hand, and given the structural exigencies of federal or EU lawmaking on the other, state regulation presents a compelling, if temporary,[55] response to the privacy conundrum.

Therefore, if Brandeis's dissent is taken to heart, and "...[t]here must be power in the states and the nation to remold, through experimentation,... economic practices and

[51] "...we start with the assumption that the historic police powers of the States were not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress...", *Rice v Santa Fe Elevator Corp.* 331 US 218 (1947). *See* Ernest A. Young, *The Ordinary Diet of The Law: The Presumption Against Preemption in the Roberts Court*, SUP. CT. REV. 253 (2011) (trying to rationalize the Supreme Court's case law on preemption, otherwise categorized as a "muddle").

[52] *See supra* note 33.

[53] *New State Ice Co. v. Liebmann*, 285 U.S. 262 (1932) (Brandeis, J., dissenting).

[54] *See supra* note 32, Ernest A. Young.

[55] *See* e.g. BJ Ard, *The Limits of Industry-Specific Privacy Law*, forthcoming, IDAHO L. REV. (2015) (discussing the deficiencies of quickly enacted state laws such as the California Reader Privacy Act).

institutions to meet changing social and economic needs," then preemption, "the boogeyman of public interest regulation,"[56] has to be restricted in data privacy too.[57] In the US, industry's push of Congress toward the establishment of weak legislation vis-à-vis private sector regulation, also referred to as "defensive preemption,"[58] has given rise to justified fears of the centralization of privacy policies in the past.[59] Similarly, ahead of the European Commission's proposal for an EU-wide General Data Protection Regulation, American but also European businesses[60] have actively lobbied to further harmonize the existing EU law framework, a fact interpreted by some as a harbinger of lowering existing privacy protections.[61] As Professor Hills writes, "federal regulation is frequently the result of lobbying efforts by industry interests that oppose regulation. The apparent paradox of this statement dissolves when one takes into account the desire of industry for uniformity of regulation."[62] But what of "defensive preemption"? Consider this scenario: when enabled, independent state models develop autonomously, although not in isolation. Horizontal interaction and spillovers between the state jurisdictions create a dynamic of horizontal adaptation between states and institutions.[63] This dynamic, even if powerful, does not result in full harmonization but is likely to facilitate "races to the top" in the private sector too. If the federal government or the EU legislator refrain from preempting state law for a period of time, at least some of the higher standards of consumer or

[56] Kirsten H. Engel, *Harnessing the Benefits of Dynamic Federalism in Environmental Law*, 56 EMORY L. J. 159, 163 (2006).

[57] *See Supra* note 23.

[58] Donald Elliott, Bruce Ackerman, and John Millian, *Toward a Theory of Statutory Evolution: The Federalization of Environmental Law*, 1 JOURNAL OF LAW, ECONOMICS, ORGANIZATION (1985), 313.

[59] In particular, regarding the CAN-SPAM ACT of 2003. *See* Roger A. Ford, *Preemption of State Spam Laws by the Federal Can-Spam Act*, 72 CHICAGO L. REV. 355 (2005) and Lily Zhang, *The CAN-SPAM Act: An Insufficient Response to the Growing Spam Problem*, 20 BERKLEY TECH. L. J. 301 (2005).

[60] "Today European enterprises support harmonization and it is their dissatisfaction with the current diverging national rules that has been a main impetus in the choice of a regulation instead of a directive. From a historic point of view, it is interesting that back in the 1990s the attitude was quite the opposite. Enterprises argued strongly against harmonization and this was a main reason for the failure of the first proposed directive (1990) and the enactment of the current directive. The times have been changing." Peter Blume, *Will it be a better world? The Proposed EU Data Protection Regulation*, 3 INTERN. DATA PRIVACY L. 130 (2012). American businesses, and in particular Google, were similarly lobbying the EU Commission for harmonization.

[61] Jan Philipp Albrecht, *No EU Data Protection Standard Below the Level of 1995*, 1 EUR. DATA PROTECTION L. REV. 3 (2015) (discussing attempts of some EU member state governments lobbied by industries to weaken the principles of data limitation and data minimization three years after the original draft regulation was tabled but also asserting the determination of the EU Parliament to block such attempts in the legislative process).

[62] *See supra* note 48, Roderick Hills Jr.

[63] *See supra* note 48, Heather K. Gerken & Ari Holtzblatt.

fundamental rights protection introduced in at least some of the states are likely to be voluntarily taken up by the industry. This would then minimize "defensive preemption," as the starting point for negotiations of a new federal or EU-wide regulation would be driven beyond a point where its impact on individuals might be arbitrary. Think of data breach notification or student privacy laws, as well as location tracking practices in the US, where at present there is no comprehensive federal statute but various divergent statutes in the states.[64] Several targeted expert interviews with privacy litigators and chief privacy officers of representative major US interstate businesses, as well as amici briefs submitted by leading national telecommunication companies reveal a certain pattern. For reasons of consistency and uniformity in consumers' treatment but also in order to avoid legal challenges in potential cross-border lawsuits, and to save costs from developing technologically differentiated products or services, in cases of multiple jurisdictions that pose different requirements, some businesses tend to voluntarily adopt the higher standard. Since uniformity is beneficial for industry, once there is a need for privacy protection spurred by new technological developments and a perceived lack of clarity among the divergent state laws, the federal legislator or agency, i.e., the FTC or the Consumer Financial Protection Bureau (CFPB), can step in and evaluate which strategies were successful in the states and which were less so. Since industry is more willing to accept centralized regulation or even actively lobby for such, and given that "first mover" states have managed to disseminate a higher standard among at least some important industry players, the incentives for businesses to insist on significantly lowering a standard on the federal or the EU level dwindle. This is partly because some businesses have already conformed to the higher standard and partly because the higher standard has become embedded into their business models. Such companies might favor centralizing data privacy legislation around the higher bar in order to achieve a level playing field with their competitors. The federal or EU lawmaker could capitalize on such developments when standardizing privacy laws. To be sure, given the compromise-driven nature of US federal and EU lawmaking, as well as the strong temporal dimension in this area of the law, the space to maneuver for the federal or EU law policymaker is hardly unlimited. Ultimately, either in conjunction with preserving features pertinent to

[64] *See infra pp.* 20-22, 24-26 and 43-44.

(member) states' national identities (when such identities can later become a part of federal or EU identity), or based on a theory that allows state experimentation[65] to be stimulated for a period of time, a judicial "presumption against preemption" in data privacy regulation[66] seems like a necessary safety valve against ossification. Moreover, a one-size-fits-all approach is sometimes both unfeasible and undesirable: hence, some state standards are best left to the states.

State institutions have a role to play in that story, too: influencing both the public and the private sector, they catalyze change. Much as data privacy has a life cycle presenting an array of potential harms that can vary when the data is being collected, processed, disseminated or intruded upon, [31] different state institutions have different levels of involvement and input at the different stages of the privacy policy-making cycle in (quasi)-federated systems. In the US, the state legislatures and attorneys general are becoming privacy agenda-setters and enforcers, while the state supreme courts oppose practices of warrantless search, offering arguments that can help replace current precedents at the Supreme Court. In the EU, the national parliaments are given a voice in EU privacy lawmaking, and data protection authorities' important involvement in its implementation might even be reinforced with the reformed law. At the same time, the EU national constitutional courts have already quashed the implementation of security enhancing measures that lack privacy protection. By defying the status quo, state institutions help safeguard privacy federalism: they guard against ossification while allowing for a level of centralization and consolidation of data privacy to the benefit of individuals, businesses and law enforcement alike. Next, I examine these insights by looking into the interaction of state institutions and regulatory models with the federal

[65] Such an approach in the EU, however, would not tolerate national legislation to experiment with surveillance once national measures go beyond the protection set out in the EU Charter. *See e.g.* Alissa J. Rubin, *Lawmakers in France Move to Vastly Expand Surveillance*, N.Y. TIMES, May 5, 2015, *available at: http://www.nytimes.com/2015/05/06/world/europe/french-legislators-approve-sweeping-intelligence-bill.html?_r=0*. It can be argued that the proposed French law that would allow the intelligence services bulk data collection and analysis of metadata would fall within the scope of the EU Charter and might be declared incompatible with it.

[66] For steps in the right direction, albeit in a rather uncontroversial case, *see Am. Bankers Ass'n v. Lockyer, 2004 U.S. Dist. LEXIS 12367* (E.D. Cal. June 30, 2004), appeal docketed, No. 04-0778 (9th Cir. June 30, 2004). Although financial institutions have asserted that FCRA preempts affiliate information sharing for non-marketing solicitation purposes, the federal district court upheld California's financial privacy law.

level and the concurrent role of industry in aspects of US consumer privacy and law enforcement.

II. THE SAFEGUARDS OF PRIVACY FEDERALISM IN THE US AND THE EU

1. The Role of State Legislatures in Consumer Privacy in the US

In the absence of a comprehensive federal approach to data privacy in the US, the states have long stood at the forefront of privacy policies. Unlike the Federal Constitution, several states explicitly enshrine the right to privacy in their constitutions.[67] Surprisingly, scholarly attempts to systematize the hodgepodge of state legislative and policy initiatives and their impact on federal level developments are rare.[68] The relationship of state to federal regulation in data privacy can be divided into three main categories: first, state privacy laws that have yet to be attempted at the federal level; second, state statutes that have begun to be canvassed by the federal government; and third, state statutes that go beyond the already existing federal standard of protection. [69]

The employment sector falls within the first group of state regulations without a federal analogue (or without any attempt at such thus far). Ten states have enacted bills protecting the private social media accounts of employees since 2013, beginning with Arkansas, Colorado, Illinois, Nevada, New Jersey, New Mexico, Oregon, Utah, Vermont and Washington; at least twelve other states are in the process of enacting or considering

[67] According to the California Constitution: "All people are by their nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." CAL. CONST., art. I, § 1. The Alaska Constitution provides: "The right of the people to privacy is recognized and shall not be infringed." ALASKA CONST, art. I, 11 § 22. Unlike the U.S. Constitution and most state constitutions in the US, but similarly to how privacy is protected in the EU Charter of Fundamental Rights and in the European Member State constitutions, California's constitutional right to privacy applies not only to state actors, but also to private parties. See Sheehan v. San Francisco 49ers, 201 P.3d 479 (Cal. 2009); Hill v. NCAA, 865 P.2d 638 (Cal. 1994).

[68] For the exception that proves the rule *see supra* notes 21 and 23.

[69] A fourth category might encompass state resistance to centripetal trends. *See* Priscilla M. Regan & Christopher J. Deering, *State Opposition to REAL ID*, 39 PUBLIUS, 476 (2009) (documenting state legislative initiatives against the Real ID Act and analyzing possible motivations for state resistance from a political science perspective). For the response of state courts opposing federal or EU surveillance legislation, *see infra pp.* 53-58.

similar laws at the moment of writing.[70] State legislatures have navigated around the preemption provisions of the Fair Credit Reporting Act (FCRA) in order to modernize and ameliorate employment opportunities for constituents with criminal records often incurred decades ago, as well as to tackle issues related to identity theft problems and the inclusion of medical debt in consumer reports.[71] Apart from the widespread problem of inaccuracy in credit records, even accurate credit reports may unduly blacklist otherwise well-qualified job candidates by drawing the attention of the employer to often irrelevant information. In Hawaii, Massachusetts, Rhode Island, and Minnesota the state legislatures have prohibited companies from asking job candidates up-front if they have a criminal record (the so-called "ban-the-box" laws), and Illinois and Washington DC are expected to sign similar bills.[72]

As mentioned above, data breach notification laws fall in the second category. Since 2002, when the first such law was enacted in California,[73] forty-seven other states have put in place laws of a similar kind.[74] The Democratic leadership wanted to enact a data breach notification legislation reflecting California law in the 112th Congress, but the initiative was abandoned likely due to gridlock until President Obama renewed his call in 2015.[75] Questions of where exactly to set the federal standard on breach notification now abound. In the negotiations, the federal lawmaker should take into account the expertise of privacy lawyers arguing that:

---

[70] For a summary of state bills, *see* National Conference of State Legislatures, *Access to Social Media Usernames and Passwords*, http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx, (last visited Apr. 28, 2015). *See also* JAMES B. JACOBS, THE ETERNAL CRIMINAL RECORD 37-38 (2015).

[71] *See* Elizabeth D. De Armond, *Preventing Preemption: Finding Space for States to Regulate Consumers' Credit Reports*, (forthcoming, 2015) (documenting the shortcomings of FCRA and charting a way forward for the states to regulate shoulder-to-shoulder with the federal tier). *See also* Gail Hillebrand, *After the FACTA: State Power to Prevent Identity Theft*, 17 LOY. CONSUMER L. REV. (2004) (analyzing FCRA's preemption provisions after the additions made in 2003 by the Fair and Accurate Credit Transactions Act (FACTA) of 2003 and arguing that the states retain significant regulatory control).

[72] Pam Fessler, *How Banning One Question Could Help Ex-Offenders Land A Job*, available at: http://www.npr.org/2014/07/14/330731820/how-banning-one-question-could-help-ex-offenders-land-a-job.

[73] CAL. CIV. C. §§ 1798.29, 1798.82 (West Supp. 2009).

[74] *See supra* note 28. *See also* Dana Lesemann, *Once More unto the Breach: An Analysis of Legal, Technological and Policy Issues Involving Data Breach Notification Statutes* 4 (2012) AKRON INTELL. PROP. J. 203 (categorizing state breach notification laws into two main models based on strict liability or risk assessment).

[75] *See* White House Proposal on Personal Data Notification & Protection Act of 2015, https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf (last visited Apr. 28, 2015).

> ...many companies that have been subject to data breaches involving multiple states have chosen to provide notice in a manner that is compliant with the statute with the strictest or most detailed state breach notification law. The reasons for this tend to be: (1) consistency in the content and timing of notices, (2) uniformity in the treatment of consumers, regardless of their state of residence, (3) perceived 'safety' on erring on the side of providing notice to all affected individuals and including more detail in such notices and (4) simplicity and economy is sending out one or two forms of notice rather than 20, 30, etc. Where a breach affects residents of states that have a 'harm threshold' as well as residents where there is a lower or no such 'harm threshold', I think most businesses (based on my experience) will provide notice to all affected individuals even where there might be a technical legal argument that notice is not required in all the affected states....[76]

Further insights from interviews with representative interstate industries and members of a Washington DC-based think-tank, the *Future of Privacy Forum* (FPF) Advisory Board,[77] reveal similar insights:

> A few years back, there was a lot of angst among companies about the divergence in breach notification statutes in the states. Certainly, most of the businesses have been taking up the higher bar especially after the ChoicePoint incident when, after the breach, ChoicePoint only alerted victims in California since it was legally obliged to give notification there. Narrowly adhering to legal obligations in this sense generally creates bad PR. The momentum for a federal statute on breach notifications might have been lost, however: there was a feeling of urgency and the push was harder 5 – 6 years ago. Over time, companies have learnt to live with the divergent statutes...[78]

There are two separate issues when it comes to breach notification statutes: what to do

[76] E-mail interview with partner in a law firm specializing in privacy litigation (Feb. 15, 2015).

[77] About one-hundred leading US companies are part of the Future of Privacy's (FPF) Advisory Board. *See http://www.futureofprivacy.org/about/our-mission/*. All interviews were anonymous.

[78] Telephone interview with a Chief Privacy Council from a company member of the FPF (June 24, 2015).

before the breach and what to do after. A risk-based approach, which seems to be the one espoused by most companies, weighs in the costs of encryption against the costs provoked by compensating mechanisms. What is protected under state laws, as a baseline, is reasonable encryption. Hypothetically speaking, if one state adopts a very prescriptive form of encryption, it is unlikely that such a statute would exert a lot of influence outside its jurisdiction. However, it is absolutely true that efficiency is important given state law inconsistencies that create compliance problems: how to notify and who....If one statute scheme covers around 85% of the requirements in the other states, companies may prefer to follow that statute. That way, even if an attorney general decides to start an enforcement action and a company is not 100% in compliance, the attorney general might take into account that the company in question is complying with the spirit of the law. And yes, California has certainly been a leader in that area and it is also where we are based... When considering the necessity of a federal bill, one has to keep in mind that wide variations in the forty-seven different state breach notification statutes will continue to exist. The way personally identifiable information (PII) is defined continues to change in the states: what used to be an account number and a name is now [in state law] often [including] an e-mail address too....[79]

The trend of adopting the higher standard in breach notifications is certainly not uniform. Another interviewee shared that:

> Companies do not deicide to standardize in a one-dimensional sort of way....My company has preferred to deal with breach notifications on a one-off basis instead of adopting a single standard. The current status quo of conflicting standards is not preferable, though. We have only so much "peanut butter" to go around with, after all....so we might want to standardize depending on what the alternative is...Every day there are attempted breaches but what is the degree of certainty we need to have to give a notification?...All in all, a federal proposal that includes preemption and reasonable triggers [such as the current one presented by the White House]

[79] Telephone interview with a Chief Privacy Council in a company member of the FPF (June 26, 2015). *See e.g.* CAL. CIV. CODE § 1798.29(g)(2) (2014) (expanding California's definition of PII to include username and password). In addition, the same interviewee added that: "FCRA and GLBA have certainly allowed for state variations too but the differences are not that big of a deal, at least for my industry. It might be that this is so because the federal standard has come in first."

can be a good starting point for negotiation.[80]

Clearly, in some sense preemption remains the preferred default for businesses but the question remains whether, based on a cost-benefit analysis, the industry might be ready to accept a compromise that would allow for a relatively high federal standard. It should be noted that the government has already managed to set a limited nationwide data breach notification obligation for health care information covered by federal health privacy law.[81] Ultimately, as one of the industry representatives mentioned, there is no way that businesses can reap the benefits of regulation without incurring *some* cost.[82]

Even more controversial has been California's 2014 minor protection privacy law requiring websites to give minors the possibility to erase information that they had posted on websites.[83] The law defined minors as under the age of eighteen and not under the age of thirteen like the federal Children's Online Privacy Protection Act (COPPA) does, and outright forbade providers from marketing to minors certain products, including alcohol, firearms, cigarettes, tattoos and tanning devices.[84] The bill seems to have inspired the 'Do Not Track Kids Act' of 2011, 2013 and 2015 – thus far, unsuccessful federal legislative proposals aimed at expanding the scope of COPPA against the collection of personal or geo-location information from children and minors, and redefining "minor" as an individual over the age of twelve and under the age of fifteen.[85] To be sure, the state-to-federal dynamic has not been a one-way street, since causality can run also in the other direction: for instance, California might have been influenced by earlier efforts of the FTC regarding COPPA. New FTC guidelines or reinterpretation of federal statutory legislation can thus feed back into the policy debates underway in the states, prompting and reinforcing processes there. For instance, since 2010 the FTC had reviewed COPPA to ensure the introduction of updates in line with "evolving technology and changes in the way children use and access the Internet, including the increased use of mobile devices

[80] Telephone interview with a Chief Privacy Officer in a company member of the FPF (Apr. 29, 2015).

[81] Health Information Technology for Economic and Clinical Health Act (HITECH) 42 U.S.C.A. § 17902 (2009), Section 13407, as implemented and enforced by the FTC. *See* also the HIPAA Breach Notification Rule, 45 CFR Sections 164.400-414 that requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

[82] *See supra* note 79.

[83] CAL. BUS. & PROF. CODE 568 Privacy: Internet: minors (2013-2014).

[84] *Id*., Chapter 22.1 (commencing with Section 22580) added to Division 8 of CAL. BUS. & PROF. CODE.

[85] S. 1563, 113th CONG. and H.R. 2734, (2015).

and social networking".[86] Although the changes did not concern an increase in the age threshold as in the California bill, the list of PII that cannot be collected without parental notice and consent was expanded on the federal level to include geo-location information, photographs and videos (through the soft law mechanism prompted in FTC's guidelines). Among other elements, the security measures for websites that release children information were strengthened and covered website operators were required to adopt reasonable procedures for data retention and deletion.[87] Facebook's policies were challenged in California on the grounds of misusing users' personal data by sharing it with third parties for the purposes of behavioral advertising in a now pending class action in which Facebook tried to reach a settlement.[88.] A number of class members objected to the terms of the settlement, arguing that Facebook did not ensure valid parental consent to a minor's participation in sponsored stories. The district court dismissed that objection in part because, in its view, the federal statute preempted state law.[89] However, in the case of *Jo Batman v. Facebook, Inc.*, now pending before the Ninth Circuit Court of Appeals, the FTC submitted a neutral amicus brief to oppose that view of federal preemption.[90] The FTC argued that: "Nothing in COPPA's language, structure, or legislative history indicates that Congress intended for that law to preempt state law privacy protections for people outside of COPPA's coverage, including teenagers." In an expression of cooperative federalism, the federal tier represented by the FTC has tried to reinforce a state legislative initiative, which in turn can at some point seep at the federal level.

Again in California, the legislature in 2014 passed a package of bills that protect student privacy. The Student Online Personal Information Protection Act (SOPIPIA) prohibits online operators from compiling profiles on students for purposes other than those for which the information was originally collected; even if those operators do not contract with educational agencies, they cannot sell students' information or target

---

[86] I am grateful to Ira Rubenstein for pressing me on this point. F.T.C. CONSUMER PROTECTION BUREAU, FTC STRENGTHENS KIDS' PRIVACY, GIVES PARENTS GREATER CONTROL OVER THEIR INFORMATION BY AMENDING CHILDREN'S ONLINE PRIVACY PROTECTION RULE https://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over (2012) (last visited Jul. 19, 2015).

[87] *Id.*

[88] Fraley ex rel. Duval v. Facebook, Inc., Case No. 11-CV-01726 LHK (PSG).

[89] [COPPA may] "bar any efforts by plaintiffs to use state law to impose a parental consent requirement for minors over the age of 13", *Id.*

[90] Amicus brief in Support of Neither Party No. 13-16819, FTC, March 20, 2014.

advertising on their website or any other website using information acquired from students.[91] Moreover, local educational agencies that adopt a program, which gathers in its records pupil information obtained from social media, need to first notify the students and their parents about the proposed program, and to provide an opportunity for public comment at a regularly scheduled public meeting before such programs are adopted.[92] Having the California bill as a point of reference[93] and in the wake of public outcry regarding the lack of any privacy protection in the growing use of education software,[94] representatives Luke Messer, a Republican from Indiana and Jared Polis, a Democrat from Colorado, introduced the Student Digital Privacy and Parental Rights Act of 2015 that is aimed at closing some of the flagrant loopholes.[95] Companies active in student software provision shared that:

> There is a lot of activity on the state level in this area and we try to support it. In general, we are supportive of a lot of privacy legislation because company practices are one thing but the lack of baseline legislation hurts everybody, it hurts trust...Congress can build up on the state legislative activities on student privacy, there are enough state statues by now: basically, with student privacy we are at a point that resembles the dynamics with breach notification statutes a few years back. It would be interesting to see whether the opportunity [for a federal statute] is seized within the next few years...In terms of the state laws, the first few set a relatively low bar of protection. SOPIPA is relatively more protective and since other states and industries *de facto* are starting to follow it, it may provide a good

[91] CAL. SOPIPA, S. B. 1177. *See also* CAL. A. B. 1442. More generally, *see* A. B. 1584 that provides for the local educational agency to maintain and control student records. Students can keep control of content created for school purposes, along with a way to transfer their information to a personal account later, *id*.

[92] Also Arizona, Colorado, Idaho, Oklahoma, New York and Rhode Island have introduced variations of student privacy regulations that either require K-12 schools to contractually oblige vendors to safeguard student privacy and security, prohibit secondary uses of student data without parental consent or introduce measures for the collection and use of pupil data, *see* NATIONAL CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research/education/student-data-privacy.aspx (last visited Jul. 19, 2015).

[93] For a comparison of relevant provisions of SOPIPA with the proposed in 2015 Polis-Messer federal bill and a voluntary code of conduct, *see Brenda Leong, Future of Privacy Forum*, http://www.futureofprivacy.org/wp-content/uploads/Pledge_CA_House032015-comparison.pdf)(last visited Jul. 19, 2015).

[94] Joel Reidenberg, N. Cameron, Jordon Kovnot, Thomas B. Norton, Ryan Cloutier, and Daniela Alvarado, *Privacy and Cloud Computing in Public Schools*, Center on Law and Information Policy (2013).

[95] H.R. 2092, 114th Cong. (2015).

base for a new federal law.[96]

and

> We just cannot keep up with all the state laws even if we try...Some of the proposed state legislation is too restrictive, for instance Louisiana has just tabled a new law that completely prohibits the sharing of student data.[97] This actually means that a school in Louisiana can not legally provide the names of the students that a public or private entity is contracted to provide services for, including bus companies, special education service providers and many more. It also makes it illegal for high schools to provide information to universities that may offer scholarships to their students. They are working on fixing the bill but have not...We are active in about twenty states but cannot afford lobbying across the country to go about fixing such bills... SOPIPA has some irrelevancies too: for example, it only applies to external vendors and it does not impose penalties for school districts that are in violation of the law. This is an expensive rule and creates competition issues for us...What is more, the problem is that SOPIPA only refers to K-12 school purposes: it does not cover post-secondary education. As a company, we would prefer a consistent set of rules for education. People, too, really want to have control over their information and to know what it is used for. The Family Educational Rights and Privacy Act (FERPA) fails to impose strong penalties and is generally not a good mechanism to go for since it does not give to students or parents control over PII.[98] For example, FRPA [currently] does not offer the possibility for copying and downloading student information. The suggestion of the Department of Commerce some time

[96] *See supra* note 77.

[97] LA. H.B. 946 (2014) http://www.legis.la.gov/legis/ViewDocument.aspx?d=880375&n=HB946%20Original (last visited Jul. 19, 2015).

[98] Senators Edward Markey, a Democrat from Massachusetts and Orrin Hatch, a Republican from Utah, proposed some amendments to the Family Educational Rights and Privacy Act (FERPA) already in July 2014. A different FRPA amendment proposal of 2015 (by John Kline, a Republican from Minnesota and Robert Scott, a Democrat from Virginia) might be one of the most robust to date. Aiming to complement the Polis-Messer proposal, it expands the definition of student education record and holds that under threat of fines of up to $ 500, 000, schools, as well as local and state education mechanisms are required to not provide to third parties access to student data for marketing and advertising purposes; it also gives access and correction rights to parents and introduces the possibility for opt-outs of certain uses of data. *See* H.R. Discussion Draft to Amend the General Educations Provisions Act, 114th Cong, (2015).

> ago to fine companies but not the school districts and the non-profit sector is unworkable as well...Generally, a federal statute that provides control mechanism, consistency and coverage for school districts and non-profit organizations (who are often the ones actually selling students' data!) can be a plus. Higher privacy standards are actually beneficial for folks like us: we are supporting economies of scale, this is good for us, and it's good for education...But everyone has to do it...[99]

The FTC also weighed in the process by updating its guidelines for student data privacy in March 2015.[100] Although clearly less strict, the FTC guidelines draw on California's package.

Finally, a third category of state legislation goes above the federal floor. Whereas the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) establish data security requirements for the organizations that fall under their jurisdiction, and the FTC enforcement actions work to the same effect even in the absence of a security leak, some states have innovated further. Currently twenty-six states[101] have legislation in place mandating the destruction of personal information, with California and Massachusetts establishing substantive requirements in that regard: under Massachusetts law,[102] for example, covered entities need to provide security programs with specific technical, administrative and physical safeguards. Whereas one of the chief privacy officers I interviewed shared that their company on its own initiative complies in

[99] Telephone interview with a founder of a company member of the FPF (June 24, 2015).

[100] Based on the Children's Online Privacy Protection Act (COPPA), a school district may act as a parent's agent providing consent to the collection of children's information on the parent's behalf, as long as the consent is limited to the educational context. The FTC recommended as best practices that parents are allowed to review the personal information collected and that operators delete children's personal information once it is no longer needed for educational purposes. In addition, schools have to provide notice of right to opt-out to parents that can opt their children out of participation in activities involving the collection, disclosure, or use of personal information collected from students for the purpose of marketing or sale to third parties. FTC FAQ, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Schools (2015)(last visited Jul. 19, 2015). One of the interviewees further hoped that student software will soon be standardized across the US because: "there is need for consistency on the one hand, and there is political salience, on the other...We do one-off deals with the schools now but this is becoming too hard to manage. The FTC's guidelines on the subject, although they do not exactly specify which projects are in and which are out, are altogether solid and can serve as a first draft for federal legislation. California's standards for kids' protection might be going too far, however...but we are complying within their jurisdiction, trying to achieve local accommodation whenever possible...", *see supra* note 79.

[101] *See supra* note 21.

[102] MASS. CODE REGS. § 17.00 (2011).

all states with the Massachusetts standard as "it substantively makes sense",[103] another interviewee shared that:

> State breach notification laws are probably the primary example of how state laws have driven national data privacy practices for businesses (in particular large, nation-wide businesses). Other influential developments include the 2010 Massachusetts data security regulation, which at the time it was enacted was the most detailed regulation addressing administrative and technical security measures. A handful of other states have followed that regulation to some extent, but, again, Massachusetts became a sort of *de facto* data security standard for some businesses. Many data services contracts, such as in outsourcing, reflect the influence of that regulation by referencing the regulation. That sort of practice is another example of how state laws have 'moved the needle' in corporate security practices. [104]

Other representatives of corporate entities shared that: "...even if we don't do business in Massachusetts, we try to keep up with that standard..."[105] and "...my sense is that this statute did set a default standard then: you cannot build security only for Massachusetts; however, industry mandates for encryption have significantly surpassed the Massachusetts standard since..." [106], especially given that "...the health and financial sectors are already regulated by HIPAA and GLBA, and European and Canadian laws have played a role, too..."[107]

2. The Role of State Attorneys General for Consumer Privacy in the US

State attorneys general play an active role in the promotion and institutionalization of such privacy-friendly initiatives in the US states. As Professor Paul Schwartz has remarked, attorneys general are elected officials and as such, are typically motivated to act upon "hot-button" issues that receive media attention.[75] Kamala Harris, California's

[103] *See supra* note 79.
[104] *See supra* note 75.
[105] *See supra* note 98. *See also* Jared A. Harshbarger, *Cloud Computing Providers and Data Security Law: Building Trust with United States Companies*, J. TECH. L. & POL.'Y (2011) "...it is apparent that this Massachusetts law has brought together many of the elements of its federal and state predecessors to compose the most comprehensive data security regulation for cloud providers..."
[106] *See supra* note 78.
[107] *Id*.

Attorney General (now running for a Senate seat), and her special assistant Attorney General Travis LeBlanc, now heading the Federal Communications Commission (FCC) Enforcement Bureau, have played a decisive role in establishing a new Privacy Enforcement and Protection Unit in California and doubling the number of prosecutors protecting privacy enforcement of state and federal privacy laws in their state. What is more, in 2012 Harris entered into an agreement with major industry players such as Google, Microsoft, Apple, Amazon.com, Hewlett-Packard, Research-In-Motion and later Facebook, requiring these companies to adopt privacy policies for their mobile applications (apps) in order to comply with California's Online Privacy Protection Act (CalOPPA).[108] Privacy policy adoption in mobile applications leapt from 19 percent in 2011 to 72 percent in 2013[109] while, Harris, interpreting broadly CalOPPA, made sure to commence enforcement actions against those companies that had not yet put such policies in place. Further, next to initiating the changes in California's minors' privacy protection law, the California Attorney General has also sponsored the "Do Not Track" amendment to CalOPPA requiring that companies collecting "personally identifiable information about an individual consumer's online activities over time and across third party web sites or online services" must disclose how they respond to browser "do not track" signals or "other mechanisms that provide consumers the ability to exercise choice regarding such collection."[110]

In addition to becoming agenda-setters on their own accord, it should be noted that the attorneys general are given statutory enforcement powers under both federal and

[108] The CalOPPA requires operators of commercial websites that collect data from Californian residents to detail the kinds of information gathered by the website, how the information may be shared with other parties, and, if such a process exists, describe the process that the user can use to review and make changes to their stored information. In order for the act to have teeth, it has been designed to have a broad scope going well beyond California's borders: neither the web server nor the company that created the web site has to be in California to fall under the scope of the law. CAL. BUS. & PROF. CODE, Sections 22575-22579 (2004).

[109] Ganka Hadjipetrova & Hannah G. Poteat, *States are Coming to the Fore of Privacy Policies*, 6 LANDSLIDE, 12 (2014).

[110] *See supra* note 108. One of my interviewees shared that: "California's new...'Do Not Track' [requirement] and the so-called 'right to be forgotten' [for minors] will influence nationwide businesses notwithstanding the [current] lack of any comparable federal law or regulation in the US." Another example of potential state impact on federal-wide standards the interviewee gave was the detailed guidance California and other states provided on privacy disclosures in mobile devices and mobile apps, *see supra* note 75. Another interviewee largely agreed, adding that legislation focusing on transparency such as the Californian "Do Not Track" rule or the requirement to include privacy policies on mobile apps are "not too costly, a fact facilitating [nationwide] compliance for their company", *see supra* note 79.

state law,[111]– powers that they have exercised individually, for the sake of their own state, but also collectively – in cross-border actions, in conjunction with other attorneys general. In 2013 the attorney general offices of thirty seven states and the District of Columbia signed a $17 million settlement with Google after allegations that it circumvented Safari's default privacy settings and allowed third parties to track the browsers of users without their knowledge or consent.[112] Moreover, in another multistate settlement, Google agreed to pay $7 million for improper collection of personal information through its Street View project.[113] As a part of the settlements, Google has committed itself to educating its employees on privacy protection and to executing proactive monitoring of employees' actions. In 2013, Doug Gansler, the president of the National Association of Attorneys General – an established forum for attorneys general in the US – declared privacy a central issue through the NAAG's Presidential Initiative called "Data Privacy in the Digital Age".[114] Professor Judith Resnik has emphasized the significance of such "translocal organizations of government officials": "generally organized not by an interest (such as climate control or women's rights) but by the political units of this federation - by the level of jurisdiction (federal, state, county, city) or the kind of office (governor, attorney general, legislator, mayor)," voluntary organizations like NAAG or the National Conference of State Legislatures contribute to interweave the strings of the US (privacy) federalism grid. State Attorney Generals are also synchronizing their actions to send comments to federal lawmakers, as in a recent letter forty-seven NAAG members sent to Congress in order to express their views on the previously discussed federal data security and breach notification proposals.[115] Such input could be valuable and perhaps appreciated to an even greater extent if attorneys general are invited to testify in Congress on tabled legislative data privacy bills.

---

[111]On the federal level, the Attorneys General have enforcement powers under the CAN-SPAM Act, COPPA, FCRA, HIPAA and the Telephone Consumer Protection Act, *see supra* note 21. Bernard Nash, Anne-Marie Luciano and Bryan Mosca, *Recent Developments in State Attorneys General Enforcement* 46 URB. LAW. 901, 906-907 (2014), (enlisting seventeen data breach notification statutes that require notice to the AG and pointing to examples of successful actions brought by individual AGs under state statutes).

[112] *See supra* note 109.

[113] *Id*., *see also supra* Nash, Luciano and Mosca, note 111.

[114] NATIONAL ASSOCIATION OF ATTORNEYS GENERAL, 2012-2013 ANNUAL REPORT, PRIVACY IN THE DIGITAL AGE (2013).

[115] Letter from Marty Jackley, President of the National Association of Attorneys General, to the Honorable Mitch McConnell, Senate Majority Leader (Jul. 7, 2015), http://www.naag.org/assets/redesign/files/sign-on-letter/Final%20NAAG%20Data%20Breach%20Notification%20Letter.pdf.

Importantly, the state attorneys general have not only coordinated their actions horizontally but have also joined efforts with the FTC, which some argue has become "the *de facto* US data protection authority".[116] Gansler noted: "We pay close attention to [the FTC's] efforts to inform privacy policy through reports and testimony, and we keep in contact with them on enforcement matters as well." He pointed out as an example of collaboration between the FTC and his office the Maryland's Workgroup on Children's Online Privacy Protection.[117] In enforcement actions, however, state attorneys general are able to draw on what are sometimes stronger than the federal, state statutory protections. As one state regulator from California shared:

> The California Confidentiality of Medical Information Act (CMIA)[118] was not preempted by HIPAA.[119] Other states have similar health statutes although the protections might vary. When a state official [in California] considers bringing an enforcement action, they usually choose whether to bring the action under HIPAA in a federal court or under the Californian statute in a state court. In my experience, bringing a HIPAA action in a federal court is usually not the preferred option because the penalties available [under HIPAA] would be limited. Further, there are state versions of FTC's Act Section 5;[120] these are the states' unfair competition laws. The wording of the Californian one is broader than that of the federal Section 5, so for example any violation of HIPAA, CMIA or another state, or federal statute can serve as a hook to trigger California's 'baby FTC act'.[121] The advantage of this is that unlike the FTC that can only obtain injunctive relief under Section 5, our state law gives us the possibility to claim civil penalties of up to $

---

[116] Judith Resnik, *New Federalism(s): Translocal Organizations of Government Actors (TOGAs) Reshaping Boundaries, Policies and Laws, in* WHY THE LOCAL MATTERS: FEDERALISM, LOCALISM, AND PUBLIC INTEREST ADVOCACY 83, 94 (Liman Public Interest Program at Yale Law School, 2010).

[117] *See supra* note 109.

[118] CAL CIV CODE Section 56-56.07 (2005), hereinafter CMIA.

[119] The way HIPAA was designed allows for some state health laws to get exempt from preemption, sometimes even when the state provisions contradict federal law. *See* U.S Department of Health & Human Services, *Does the Rule preempt State Laws,* at http://www.hhs.gov/ocr/privacy/hipaa/faq/preemption_of_ state_law/399.html

[120] Cf. 15 U.S.C. § 45(a)(2): "The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, except banks, savings and loan institutions... from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."

[121] CAL. BUS. & PROF. CODE Section 17200: "...unfair competition shall mean and include any *unlawful*, unfair or fraudulent business act or practice", emphasis added. One such case was People v. Kaiser Foundation State Plan, Inc. (Cal. 2014).

> 2,500 for each violation (per consumer)...We collaborate with the FTC or other consumer protection agencies like the CFPB, of course, but finally, we try to do what is best for the consumer...[122]

To a certain extent and with the immediate disclaimer that unlike the European privacy enforcement authorities, both the FTC and the state attorneys general in the US are not exclusively devoted to privacy protection, the work of the US state attorneys general starts to resemble that of the national data protection authorities (DPAs) in EU countries and that of the FTC – in part, to the planned European Data Protection Board.[123] In the EU, the national data protection authorities are primarily entrusted with enforcing data protection issues, with the suggested European Supervisory Data Protection Board to be composed of representatives from the national DPAs and entrusted with the exercise of primarily coordination functions. In turn, in the US the FTC is the primacy enforcer of privacy policies but the lack of resources for regional oversight might be currently hampering its enforcement capacity: with the dynamic involvement of state attorneys general however, there might be a subtle change resulting in enhanced local oversight mechanisms for the FTC. Granted, the energy of state attorneys general on privacy matters may vary across the states whereas "windows of opportunity" for policy action remain ephemeral, with public attention on a single issue lasting only so long. On the one hand, the credibility of the comparison depends on the future coordination effort and overall involvement of the FTC that has been urged to become more assertive in new areas of privacy concern, such as Big Data.[124] On the other hand, the comparison can only hold true if the attorneys general become active in enforcing data privacy in the bank and insurance sectors too since crucially, the FTC lacks statutory powers in these areas.[125] In addition, the involvement of US state courts can be beneficial for consumer privacy in the US as well – in that regard, Maryland's Attorney General Gansler appealed to state legislators to make violation of COPPA enforceable in the state courts.[126] The enforcement

[122] Telephone interview with a state regulator from California (Jul. 15, 2015).
[123] *See infra pp.* 52.
[124] *See supra* note at 666.
[125] Under Section 5 of the FTC Act banks, savings and loan institutions, as well as federal credit unions and air carriers are excluded from FTC jurisdiction, *see* U.S.C. § 45(a)(2).
[126] *See supra* note 109.

of federal law by the state courts would reinforce the vindication of federal rights in cases where there are issues of under enforcement by the federal courts, i.e. due to lack of standing.[127]

3. Law Enforcement and the Role of State Courts in the US

The role of state courts is even more palpable in the context of US law enforcement. Some states have enacted analogues to the Fourth Amendment[128] and it might well have been that the language, logic and structure of the first such analogue – Article XIV of the Massachusetts Constitution of 1780 – foreshadowed the Federal Fourth Amendment.[129] From "Peeping Tom laws" and bans on two-way mirrors, to prohibitions on the interception of telegraph communications and on telephone wiretapping,[130] the states were also privacy frontrunners in the area of law enforcement long before the dawn of the digital era.

---

[127] ROBERT SHAPIRO, POLYPHONIC FEDERALISM: TOWARD THE PROTECTION OF FUNDAMENTAL RIGHTS (Univ. Chic. Press 2009) (making a general argument for federal rights to be claimed at state courts also in other areas).

[128] For example, the Massachusetts Constitution states: "Every subject has a right to be secure from all unreasonable searches, and seizures, of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation; and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure: and no warrant ought to be issued but in cases, and with the formalities prescribed by the laws.", MASS. DECLARATION OF RIGHTS, art. XIV. The Florida Constitution states: "Every natural person has the right to be let alone and free from government intrusions into his private life except as otherwise provided herein." FLA. CONST. art. I, §23. The California Constitution holds that: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable seizures and searches, shall not be violated.", CAL. CONST. art. I, §19. It is by no means the case that once there is a state constitutional analog, it would be interpreted differently to the Fourth Amendment: for instance, the protection granted by the Florida Constitution has been leveled to the federal one. For an overview, *see* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 Cath. U. L. Rev. 373, 427-438 (2006).

[129] Akhil R. Amar, *The Law of the Land. A Grand Tour of Our Constitutional Republic*, Basic Books: New York, p. 241. (2015). In Amar's originalist interpretation, both the Massachusetts Constitution and the Federal Fourth Amendment meant that: "warrants are heavies here, not heroes". However, warrants can be "heavies" mainly when there are general, and the Massachusetts Supreme Court in recent cases has certainly chosen to rely on specific warrants triggered by probable cause, *see infra pp.* 36, 38.

[130] South Carolina, for example, criminalizes "peep[ing] through windows, doors, or other like places, on or about the premises of another, for the purpose of spying upon or invading the privacy of the persons spied upon and any other conduct of a similar nature that tends to invade the privacy of others." S.C. CODE ANN. § 16-17-470(A) (2003); *see also* GA. CODE ANN. § 16-11-61 (2003). *See also* Daniel Solove, *A Taxonomy of Privacy*, 154 U. PENN. L. REV. 477, 491-492 (2006) (providing examples of such state laws).

The aftermath of *United States v. Jones*[131] and *Riley v. California*[132] is now giving privacy advocates reason for measured optimism regarding a possible reinterpretation of the Fourth Amendment. Before these two cases, the third party doctrine of the Supreme Court meant that under the status quo, the Amendment places no judicial restriction on information shared with a telephone provider, a bank, a search engine or any other third party to which information has been made available, even for different purposes.[133] The so-called 'third party doctrine' has been criticized for not being up to speed with new technologies, given that the Supreme Court cases that address it are all dated.[134] The mentioned two recent decisions have inspired a lively debate: some scholars favor the gradual fall into obsolescence of the doctrine, while others have focused on the workability of "a mosaic theory" under which access to information held by a third party would be limited in time and scope to avoid comprehensive profiling (while allowing law enforcement to reconcile security with privacy interests).[135]Beyond the aspirations of legal academia, civil liberties organizations have also joined forces in specifically attacking location tracking, drug prescription disclosures and drone surveillance, as these are areas of the Fourth Amendment perceived as important not only in their own right but also because of the potential they present to pierce the third party doctrine in key contexts, and perhaps lead to its gradual demise.[136]

---

[131] United States v. Jones, 132 S. Ct. 945 (2012).

[132] Riley v. California, 134 S. Ct. 2473 (2014).

[133] United States v. Miller, 425 U.S. 435, 443 (1976). Smith v. Maryland, 442 U.S. 735, 741-42 (1979).

[134] Stephen E. Henderson, *After United States v. Jones, After the Fourth Amendment Third Party Doctrine*, 14 N.C. J. L. & TECH. 431 (2013) (showing, moreover, that the Supreme Court did not apply a strong version of the third party doctrine even before *Jones*).

[135] The former argumentation has been triggered by Justice Sotomayor's concurring opinion in *Jones*, whereas the latter is based on Justice Alito's concurring opinion in the same case. *Cf.* Henderson, *id*; Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. R. 311 (2012) (arguing against the theory because of its problematic application in practice); Christopher Slobogin, *Making the Most of United States v. Jones in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST'L L. & PUB. POL'Y 1, 24 and 28 (2012) and Christopher Slobogin, *Domestic Surveillance of Public Activities and Transactions with Third Parties: Melding European and American Approaches* (forthcoming 2015) (suggesting a proportionality theory of the Fourth Amendment to apply the mosaic approach); for a similar idea *cf.* Stephen E. Henderson, *Real-time and Historic Location Surveillance after United States v. Jones: An Administrable, Mildly Mosaic Approach*, 103 J. CRIM. L. & CRIMINOLOGY 803, 820 (2013) ("[t]he threshold protection would be that a single datum of location information is not protected, a day or less of location information is moderately protected, and more than a day of location information is highly protected").

[136] Interview with an ACLU attorney, in N.Y., N.Y. (May 20, 2015). "The ACLU and other groups have certainly argued that state rejection of the third party doctrine in particular areas (both through legislation and through court decisions) should be a factor in evaluation of whether the third-party doctrine should apply to those areas under the Fourth Amendment." *Id.* Further, *cf.* amicus brief of EPIC submitted in State

State courts have an important role to play in developing this area of the law. On the one hand, the interpretation of a reasonable expectation of privacy in the digital era by state court judges may generate a snowball effect that would lead to horizontal adaptation between state jurisdictions and the private sector, and thus could then weigh on federal court judges' and legislators' interpretation of the Fourth Amendment. On the other hand, state court decisions also offer substantively compelling reasoning that prepares the ground for a possible constitutional reinterpretation or statutory legislation. In other words, state court decisions matter on a federal scale, both quantitatively and qualitatively.

In the former sense, state court interpretations of state analogues of the Fourth Amendment not only potentially add constitutional rights to the Fourth Amendment floor[137] but also are themselves relevant in defining that floor. Horizontal adaptation through state court spillovers can be discerned pre-*Jones* if one compares the Oregon Supreme Court[138] with that of the Supreme Courts of Washington,[139] New York[140] and Massachusetts:[141] all four courts quoted each other and eventually coincided in requiring law enforcement officers to be issued with a warrant before installing radio transmitters or GPS tracking devices in cars. Moreover, in requiring a warrant, state courts both pre- and post-*Jones* specifically denounced the profiling effect of location tracking and the possible dangers it presents for revealing potentially sensitive information.[142] Quoting the preceding judgments of the Supreme Courts of Washington and of Oregon, the New York judges stated: "We find persuasive the conclusions of other state courts that have addressed this issue and have held that the warrantless use of a tracking device is inconsistent with the protections guaranteed by their state constitutions".[143]

---

of New Mexico v. Norman Davis, 321 P.3d 955 (2014) (the state court found that the warrantless aerial surveillance of the defendant's greenhouse breached the New Mexico Constitution).

[137] *See* Stephen E. Henderson, *supra* note 128.

[138] State v. Campbell, 306 Or. 157, 759 P.2d 1040 (1988).

[139] State v. Jackson, 150 Wash. 2d 251, 76 P.3d 217 (2003) ("We find persuasive the analysis of the Oregon Supreme Court in a case involving a radio transmitter attached without a warrant to the exterior of a suspect's vehicle...").

[140] People v. Weaver, 12 N.Y.3d 433, (2009).

[141] Commonwealth v. Connolly, 454 Mass. 808 (2009).

[142] *Weaver*, 12 N.Y.3d at 362; *Jackson*, 150 Wash. 2d at 262-263; *Connolly*, 454 Mass. (Gants, J., concurring) and State v. Earls, 214 N.J. 564, 569 (2013) (ruling that under the New Jersey Constitution cell phone real-time location tracking three times in one day requires a warrant subject to a probable cause).

[143] *Weaver*, 12 N.Y.3d at 365-447. *Horizontal adaptation* does not mean that all state courts end up deciding on identical grounds. For instance, in location tracking cases the state courts might be divided on

As when serving to shed light on the interpretation of other constitutional rights,[144] absolute consensus among state courts and legislatures should not be dispositive inasmuch a trend among the states becomes visible: as shown in *Mapp v. Ohio*,[145] which reversed a Supreme Court precedent, it sufficed that at the time half of the states required suppression of evidence obtained via an unconstitutional search or seizure (that is, had in place an exclusionary rule) for the Supreme Court to recognize such Fourth Amendment protection. When *Jones* was being decided, the four state courts just mentioned favored restrictions on GPS tracking, while ten others did not.[146] Although on narrower grounds than those raised by the state judges,[147] this did not deter the majority in *Jones* to condemn the practice under the US Constitution. Moreover, even if the Supreme Court may be hesitant to depart from the *status quo* before a more palpable national consensus emerges,[148] there can hardly be any similar concern on the side of the federal legislator as the democratically elected lawmaker. Drawing on each other's decisions, the state courts that have reviewed cellphone location tracking post-*Jones* have thus far all ruled against giving free reign to the practice.[149] Congress can capitalize on this trend by amending the

---

whether there is a search (as in *Earls*, 214 N.J. 564) or a seizure (as in *Connolly*, 454 Mass.) under their domestic constitutions.

[144] Bilyana Petkova, *The Notion of Consensus as a Route to Democratic Adjudication?*, 14 CAMBRIDGE Y.B. EUR. LEGAL STUD. 663 (2011-2012) (discussing nuances in the application of the consensus method to fundamental rights by the ECJ, the ECtHR and the US Supreme Court).

[145] Although in Mapp v. Ohio the Supreme Court rejected reliance on state law when defining the scope of the 4th amendment, in practice it was influenced by it. Mapp v. Ohio, 367 U.S. 643 (1961).

[146] State courts that did not accord state constitutional protection for GPS location tracking pre-*Jones* include: Devega v. State, 286 Ga. 448, 689 S.E.2d 293 (2010); Stone v. State, 178 Md.App. 428, 941 A.2d 1238 (2008); Osburn v. State, 118 Nev. 323, 44 P.3d 523 (2002); People v. Gant, 9 Misc.3d 611, 802 N.Y.S.2d 839 (N.Y.Crim.Ct. 2005); State v. Johnson, 190 Ohio App.3d 750, 944 N.E.2d 270 (2010), appeal docketed, No. 2011–0033, 128 Ohio St.3d 1425, 943 N.E.2d 572 (Ohio 2011); Foltz v. Commonwealth, 57 Va.App. 68, 698 S.E.2d 281 (2010), aff'd en banc, 58 Va.App. 107, 706 S.E.2d 914 (2011); State v. Sveum, 319 Wis.2d 498, 769 N.W.2d 53 (Wis.Ct.App. 2009).

[147] Scalia's majority opinion in *Jones* decided the case under trespass theory (*Jones*, 132 S. Ct.) whereas the concurring opinions and most state courts applied the reasonable expectations of privacy test, first announced in Katz v. United States, 389 U.S. 347 (1967).

[148] Roderick Hills, Jr. *Counting States*, 32 HARV. J. L. & PUBL. POLICY 17 (2009) (arguing that the Supreme Court should at most pressure outlier states into following the course taken by the rest).

[149] *Earls*, 214 N.J.; Commonwealth v. Rousseau, 990 N.E.2d, 543, 553 (Mass. 2013) (although defendant had no possessory interest in the vehicle at issue, he had standing to challenge warrants authorizing the State police to install and monitor for a period of thirty days a GPS tracking device on vehicle in which defendant rode as a passenger); Commonwealth v. Pitt, WL 927095 (Mass. 2012) (it would be incongruous to decide the constitutionality of a search *post hoc* based on the information it produced and therefore, a warrant is necessary for real-time CSLI); State v. Zahn, 812 N.W.2d 490, 497 (S.Dak. 2012) (warrantless attachment of a GPS to defendant's vehicle for 26 days was found unlawful); Commonwealth v. Augustine, 467 Mass. 230 (2014) (the third party doctrine does not apply to compelled disclosure of CSLI and a warrant is needed instead); Tracey v. State, 152 So.3d 504 (Fla. 2014) (cell site location information

Electronic Communications Privacy Act (ECPA) (or the Stored Communications Act), or by introducing the Geolocational Privacy and Surveillance Act (GPS Act), processes already under way.[150] Certainly, this is not to say that numbers do not matter. Civil rights organizations' state affiliates have realized the importance of the states and are working on to improve the count by lobbying state legislatures to pass statutory bans on location tracking and drug prescription disclosure, as well as on surveillance drones.[151] To that effect, the American Civil Liberties Union (ACLU) has provided draft state legislative bills on location tracking that by 2014 ended up being adopted or considered for adoption in about a dozen of the states.[152]

When looking into the qualitative impact of state law, it is worth mentioning the reach it has into Supreme Court's separate opinions that can later serve as building blocks for eventual constitutional reinterpretation. State courts decide cases based on the federal Constitution or on the respective national Fourth Amendment analogues. In the latter sense, state courts' reasoning could inform the federal bench in factually similar situations, because the wording of state constitutional provisions does not often diverge significantly from the text of the Fourth Amendment.[153] For instance, California has long

---

for real time tracking was a search within the purview of the Fourth Amendment for which probable cause was required).

[150] Geolocation Privacy and Surveillance Act (GPS) of 2013, H.R. 1312, S. 639. First introduced in 2011 and then reintroduced in 2013, the Act is a bipartisan initiative that requires the government to show probable cause and obtain a warrant before acquiring the geolocational information of a U.S. person for both real-time tracking and the acquisition of records of past movements (except in emergency situations): http://www.wyden.senate.gov/news/press-releases/wyden-chaffetz-stand-up-for-privacy-with-gps-act. Cf also the Online Communications and Geolocation Protection Act H.R. 983, a similar bipartisan initiative of 2013 to modernize ECPA by requiring law enforcement to obtain a warrant for disclosure of stored e-mail and other private documents or to track the movements of a person through his or her cell phone, https://www.congress.gov/bill/113th-congress/house-bill/983.

[151] See Marc Jonathan Blitz, James Grimsley, Stephen E. Henderson & Joseph Thai, *Regulating Drones under the First and Fourth Amendments*, WM & MARY L. REV. (forthcoming 2015) (stating that, depending on how one counts, bills regulating drone flights have been proposed at the federal level and have been enacted in between thirteen and twenty-one states).

[152] Allie Bohm, *Status of Location Privacy Legislation in the States* (2014), https://www.aclu.org/blog/status-location-privacy-legislation-states?redirect=blog/technology-and-liberty-national-security/status-location-privacy-legislation-states.

[153] For example, the language of the first part of Article I, § 12 of the New York Constitution closely follows that of the Fourth Amendment: "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. The right of the people to be secure against unreasonable interception of telephone and telegraph communications shall not be violated, and ex parte orders or warrants shall issue only upon oath or affirmation that there is reasonable ground to believe that evidence of crime may be thus obtained, and identifying the particular means of communication, and particularly

challenged the third party-doctrine: a California case holding that one retains reasonable expectations of privacy with respect to one's bank records served to underpin the dissent of Justice Brennan in *Mille*r,[154] as well as the reasoning in other state jurisdictions that have since chosen to reject the majority opinion in *Miller*.[155] Justice Brennan began his dissent by holding that: "The California Supreme Court has reached a conclusion under...the Californian Constitution in the same factual situation, contrary to that reached by the Court today under the Fourth Amendment. I dissent because in my view the California Supreme Court correctly interpreted the relevant constitutional language." Similarly, Justice Sotomayor, so far the only Supreme Court Justice to indicate that she would reject the third party doctrine, also quoted a state court when penning her concurring opinion in *Jones*. In order to show the inherent dangers that uncurbed (GPS) monitoring has of revealing potentially sensitive information, even for short-term tracking, she relied on *People v. Weaver*:

> "Disclosed in [GPS] data ... will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or

---

describing the person or persons whose communications are to be intercepted and the purpose thereof." The provision as a whole was interpreted by New York state courts as identical to the Fourth Amendment of the US Constitution, cf. People v. Harris, 77 N.Y.2d 434, 437, 568 N.Y.S.2d 702, 570 N.E.2d 1051 [1991]. Admittedly, this might not be the case of other state constitutional analogues, e.g. the language of Article I, Section 7 of the Washington State Constitution can be deemed broader than that of the Fourth Amendment: "No person shall be disturbed in his private affairs, or his home invaded, without authority of law." However, what matters for the relevance of a state judgment on a federal scale is whether the *ratio dicidendi* of the case is based on the specific wording of a State Constitution or on arguments congruent with the Fourth Amendment.

[154] Justice Brennan continued to draw at length on Burrows v. Superior Court, 13 Cal.3d 238, 118 Cal. Rptr. 166, 529 P.2d 590 (1974). "...A bank customer's reasonable expectation is that, absent compulsion by legal process, the matters he reveals to the bank will be utilized by the bank only for internal banking purposes..." in order to conclude that: "to permit a police officer access to these records merely upon his request, without any judicial control as to relevancy or other traditional requirements of legal process, and to allow the evidence to be used in any subsequent criminal prosecution against a defendant, opens the door to a vast and unlimited range of very real abuses of police power." Next to the "parade of horribles" argument, Justice Brennan uses the state court decision as a stepping stone for defying the notion that privacy is restricted to the privacy of the home. Finally, he states that: "...Burrows strikingly illustrates the emerging trend among high state courts of relying upon state constitutional protections of individual liberties protections pervading counterpart provisions of the United States Constitution, but increasingly being ignored by decisions of this Court."

[155] Henderson, *supra* note 128.

church, the gay bar and on and on".[156]

Importantly, one of the groundbreaking features of *Jones* is that it reinterpreted *Katz,* reintroducing the possibility that the US Constitution could cover surveillance of public spaces, an option already rehearsed by some state supreme courts.[157] Even before *Jones*, the judges of the Washington Supreme Court bolstered their reasoning with a case from Oregon holding that:

> "[The Oregon Court] held that the question was not whether what the police learned by use of the transmitter was *exposed to public view*, but whether use of the device can be characterized as a search.... [The Oregon Court said that] the question whether an individual's privacy interests have been infringed by an act of the police cannot always be resolved by reference to the *area* at which the act is directed."[158]

This is especially true in the face of advanced technologies, which allow for exponentially cheaper ways of monitoring one's activities, thereby blurring the line between the public and the private. Along these lines, Justice Alito noted that: "[I]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. . . . Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources." [159] Before him, in *Commonwealth v. Connoly*, the judges in Massachusetts noted that citizens can reasonably expect that their "comings and goings will not be continuously and contemporaneously monitored except through physical surveillance, which requires a far greater investment of police resources and generates far less information than [GPS]

[156] *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (citing People v. Weaver 12 N.Y.3d 433, (2009)).

[157] *Cf. Campbell*, 759 P.2d; *Weaver*, 12 N.Y.3d; *Jackson*, 150 Wash. 2d. Relying on these preceding state court judgments, the Supreme Judicial Court of Massachusetts also held after *Jones* that: "[T]hese courts have rejected the Fourth Amendment emphasis on the location of the vehicle [e.g. whether or not it is on a public roadway] when the device transmits its signal and have focused instead on the privacy interest in being free from electronic surveillance, [and in the case of the Washington and Oregon Courts]...the extent to which secret electronic surveillance by government interferes with that interest." *Augustine*, 467 Mass.

[158] *Jackson*, 150 Wash. 2d, at 263-264, emphasis added.

[159] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

monitoring".[160]

Furthermore, some of the substantive arguments voiced in state courts might help the Supreme Court recalibrate its case law, and perhaps the federal legislature to introduce statutory changes that reflect the consequences of *United States v. Jones* and *Riley v. California*. Whether the third party doctrine stands or falls (and even if there are very good reasons why it should fall),[161] the Supreme Court might want to address compelling arguments made by state court judges about why and how the doctrine could be scaled down. The state courts discuss the specificities of detailed location tracking and medical prescription disclosures that isolate a sphere where the third party doctrine might not apply, for three different reasons: first, because modern location tracking techniques create unfettered possibilities for profiling citizens, either in greater detail or by supplying more sensitive information than bank records or landline telephone slips do[162] and because in these areas of information sharing the degree of affirmative, voluntary disclosure is less compared to other contexts in which the third party doctrine has traditionally applied.[163] Finally, as one state court held regarding location tracking:

> "the distinction between privacy interests in public and private spaces makes [modern location tracking] especially problematic, because [it] give[s] off signals from within both spaces, and ...the government...has no way of knowing in advance whether the [signal] will have originated from a private or public

[160] *Connolly*, 454 Mass. at 835.

[161] *Jones*, 132 S. Ct. at 956 at 957 (Sotomayor, J., concurring).

[162] "Using a [cellular telephone] to determine the location of its owner can be far more revealing than acquiring toll billing, bank, or Internet subscriber records. It is akin to using a tracking device and can function as a substitute for 24/7 surveillance without police having to confront the limits of their resources. It also involves a degree of intrusion that a reasonable person would not anticipate.... Location information gleaned from a [cellular telephone] provider can reveal not just where people go—which doctors, religious services, and stores they visit—but also the people and groups they choose to affiliate with and when they actually do so. That information cuts across a broad range of personal ties with family, friends, political groups, health care providers, and others..." *Earls*, 214 N.J at 586.

[163] "[P]atients and doctors are not voluntarily conveying information to a state substance control database. Rather, the submission of prescription information is required by law. The only way to avoid providing such information would be to forgo medical treatment or leave the state...", emphasis added. Brief for ACLU as Amicus Curiae Supporting Defendant, State v. Pyle, No. 131910379 (Utah 3rd District Court, 2015) (citing Oregon Prescription Drug Monitoring Program v. U.S. Drug Enforcement Admin, F. Supp. 2d, (2014). Cf. also "People buy [cellular telephones] to communicate with others, to use the Internet, and for a growing number of other reasons. But no one buys a [cellular telephone] to share detailed information about their whereabouts with the police." *Augustine*, 467 Mass. at 863.

location,"[164]thereby possibly encroaching on constitutionally protected areas.

The gradual extent of scaling down the third party doctrine ultimately begs the question of whether a revived common law principle of confidentiality, as informed by the practice in the states, could reintroduce the FIPP of purpose limitation into US Fourth Amendment law. For instance, attorney confidentiality is enshrined in US common law, but physician-patient privilege is not. However, forty-three states and the District of Columbia have created such protection through statutory legislation, and a number of state courts have held that individuals have a reasonable expectation of privacy in medical records under state constitutional provisions or the Fourth Amendment. Moreover, in the context of law enforcement, the ACLU counts ten states as having enacted legislation prohibiting access from records in those states' prescription monitoring programs unless the government obtains a warrant or otherwise demonstrates probable cause.[165] Beyond the traditional context of medical and legal confidentiality, state courts might extend the concept to cover broader contexts.[166]

As demonstrated, much like in the consumer privacy context, horizontal adaptation between jurisdictions plays a major role in challenging the Fourth Amendment's *status quo* in the law enforcement arena. This is aided by industry's interest in siding with the more privacy-protective standard whenever discrepancies exist between the state jurisdictions and appellate courts. For example, in 2014, AT&T received 13,629 requests for real-time cell phone location information from the government, and even more requests for historical cell phone location (CSLI) records.[167] Similarly, from 2007 to

[164] *Augustine*, 467 Mass. at 253, cf. also *Earls*, 214 N.J at 586: "Modern cell phones also blur the historical distinction between public and private areas because cell phones emit signals from both places." *Riley* opened this line of reasoning: "[h]istoric location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." *Riley*, 134 S. Ct. at 2490.

[165] Brief for ACLU as Amicus Curiae Supporting Plaintiffs, *Oregon Prescription Drug Monitoring Program*, 998 F.Supp.2d at 42-46.

[166] *Earls*, 214 N.J at 644: "users are reasonably entitled to expect confidentiality in the ever increasing level of detail that cell phones can reveal about their lives". Brief for ACLU as Amicus Curiae Supporting Defendant, *Pyle*, No. 131910379: "prescription records stored in [a substance database] are much like emails stored in an email provider's servers. For one, the entity maintaining the digital files may access them only for limited enumerated purposes."

[167] AT&T Transparency Report (2015), http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_Transparency%20Report_January_2015.pdf; Jack Balkin, *Information*

2012, Sprint/Nextel received nearly 200,000 court orders for real-time and historical cell phone location information.[168] As the industry is grappling with the mounting requests, its preference for uniformity and legal certainty is unsurprising. In a case now pending before the 11th Circuit, AT&T submitted an amicus brief in support of neither party to argue in favor of adoption of "a categorical rule", in other words, a uniform standard that would require the government to be issued a warrant upon the showing of a probable cause for obtaining historical CSLI data under Section 2703(d) of the Stored Communications Act.[169] AT&T argued that:

> "Considerable legal uncertainty surrounds the standards the government must satisfy to compel the production of location information, and achieving legal clarity is essential to protecting consumer privacy, defining the scope of legitimate law enforcement interests, and ensuring the efficient operation of companies operating in various sectors of the digital economy...."..."...where Section 2703(d) [of the Stored Communications Act] applies, it does not necessarily authorize the government to secure information under the lower, "reasonable grounds" standard, but is instead flexible enough to require the government to meet the Warrant Clause..."... "...[W]hether this Court concludes that a probable cause standard or a "reasonable grounds" standard applies in this particular case [for historical CSLI], another issue of statutory construction is whether Section 2703(d) permits the higher standard to be applied to information within its scope. The better view is that it does."[170]

Like other major interstate businesses who are confronted with a different interpretation of the applicable legal standard by the courts, AT&T has a compelling interest in "rounding up" privacy protections toward the higher standard. As more state courts come to espouse a higher standard, companies operating nationwide who want to offer the same package of services to their customers across different jurisdictions but also

---

Fiduciaries in the Digital Age, BALKINIZATION (2015), http://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html.

[168] Brief for ACLU and ACLU of North Carolina as Amici Curiae Supporting Defendant, State v. Perry (10th Cir. 2015).

[169] Brief for AT&T as Amicus Curiae Supporting Neither Party, United States v. Davis, No. 12-12928 (11th Cir. 2014).

[170] *Id.* at 4, 6, 26.

to avoid potential litigation in the face of unclear legal obligations, have begun to coalesce toward the higher standard of probable cause, first offered in some of the states.

4. The Role of National Legislatures and Data Protection Authorities in the EU

Returning to European institutional developments, national parliaments would lose their power of discretion in the implementation of data protection laws with the new Data Protection Regulation but could instead rely on leverage in the European lawmaking process. Meanwhile, the national data protection authorities would be given significant new joint responsibilities in the implementation of the Regulation.

Article 5(3) on the Treaty of the European Union currently enshrines the principle of subsidiarity, stating that the EU may act in any areas in which it shares competence with the Member States:

> "only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level".[171]

Since the entry into force of the Lisbon Treaty, the principle of subsidiarity is supplemented with a political control mechanism detailed in Protocol No. 2, the so-called "Early Warning System".[172] According to this procedure, draft legislative acts are first forwarded to national parliaments, who verify their compliance with the principle of subsidiarity. Each Member State parliament is assigned two votes, which can be divided between the parliamentary chambers in cases of bicameral parliaments. If the number of the negative votes cast does not reach a certain threshold, the Commission may take the parliamentary opinions into account at its own discretion but no further consequences are formally triggered in the legislative process.[173]

---

[171] Art. 5(3) TEU.

[172] Protocol No. 2 on the Application of the Principles of Subsidiarity and Proportionality, TEU.

[173] Conversely, if the number of votes cast exceeds one third, the proposal must then be reviewed and the Commission may decide to maintain, amend or withdraw it. In case of a simple majority of reasoned opinions objecting on grounds of subsidiarity, for a legislative draft to still be tabled, the Commission needs the European legislature (usually the European Parliament and the Council) to approve the proposal first, *id*. Based on analogies with soccer, the procedure is commonly referred to as a "yellow card".

Legislative proposals of the Commission generally provide a detailed justification regarding both subsidiarity (is this a matter for the EU or the Member States?) and proportionality (is the proposed action the best fit with respect to ends and means). While Protocol No.2 addresses the principles of subsidiarity and proportionality, the Early Warning System expressly refers to subsidiarity only.[174] Arguably, when attacking a draft not strictly on subsidiarity grounds, parliaments and parliamentary chambers use the procedure in a somewhat sparing manner, exceeding the actual powers they are given under the Treaty Protocol.[175] Rather than an exercise in the legal craft of splitting subsidiarity from proportionality or as an unequivocal mechanism[176] for assigning legislative competence to the EU and its Member States, the Early Warning Mechanism is best understood as a part of an institutional and political dialogue between the European institutions and the national legislatures.[177] In this dialogue, input from the national parliaments is not adopted unconditionally by the European legislature, but is filtered through the perspective of European institutions in an iterative and consensus-building fashion: in the case of the General Data Protection Regulation, several of the demands raised by the national parliaments were taken on board by the European Parliament in subsequent amendments on the first reading of the draft regulation.

During the early warning mechanism procedure on the proposed Data Protection Regulation, the German Bundesrat (or higher chamber), the Belgian House of Representatives, the French Senate, the Italian Chamber of Deputies, and the Swedish Parliament submitted reasoned opinions objecting to the Commission's proposal. In addition, the Czech Senate, the German Bundestag (or lower chamber), the Dutch Senate, as well as the Romanian and the Slovenian Parliaments submitted written statements

[174] *E.g.* a national parliament is invited to specify: "why it considers that the draft in question does not comply with the principle of subsidiarity", see art. 7, Protocol No.2, TEU, see supra note 172.

[175] Federico Fabbrini and Katarzyna Granat, "*Yellow card, but no foul*": *The role of the national parliaments under the subsidiarity protocol and the Commission Proposal for an EU regulation on the right to strike* 50 Common Market L. Rev. 115 (2013).

[176] The precision and objectivity of a test that neatly splits the legislative competences between the federal or quasi-federal center and the constitutive states can in fact be doubted. *See* Judith Resnik, *Federalism(s)'s Forms and Norms: Contesting Rights, De-Essentializing Jurisdictional Divides, and Temporizing Accommodations in* NOMOS LV: FEDERALISM AND SUBSIDIARITY (JAMES E. FLEMING AND JACOB T. LEVY, EDS., NEW YORK UNIV. PRESS, 2014).

[177] Davor Jancic, *The Barroso Initiative: window dressing or democracy boost*, 8 UTRECHT L. REV., 78.

commenting on the proposal and prompting concrete questions about it.[178] The number of reasoned opinions disputing the proposal on grounds of subsidiarity was insignificant in terms of erecting any legal barriers to the future adoption of the regulation, but a common thread among the opinions and statements was the Commission's choice of a legal instrument: Most of the national parliaments stated a preference for a new or amended directive over a regulation. On a related note, national parliaments were preoccupied with preserving a high level of protection on the national level, which they feared a regulation would undermine (especially in the public sector where detailed national legislation pre-dated the proposal). In something of a contradiction, the majority of the national parliaments demanded they retain legislative discretion but simultaneously called for the strengthening of common EU guarantees for data protection in international data transfers. Another frequent concern was the empowerment of the European Commission in a number of ways and the over-centralization of data protection, most notably through the proposed exercise of the European Commission's delegated powers previewed by the regulation in many of the provisions in the Commission's draft.

However, the parliaments that submitted reasoned opinions objected to the means and not the necessity of a Union act on data protection, in other words debating the 'how' and not the 'if' of the update to the EU data protection framework. Notably, many of the national parliaments stated that they agreed with the Commission on the need to take action on the European level.[179] Interestingly, the German Bundestag submitted a

[178] Belgian Chambre des Représentants, Reasoned opinion of Apr. 6, 2012 on COM (2012) 11, (Rapport fait au nom de la Commission de la Justice, DOC 53 2145/001), French Sénat, Reasoned opinion of Mar. 4, 2012 on COM (2012) 11, German Bundesrat, Reasoned opinion of Mar. 30, 2012 on COM (2012) 11, Italian Camera dei Deputati, Reasoned opinion of Apr. 4, 2013 on COM (2012) 11, Swedish Riksdag, Reasoned Opinion of Mar. 22, 2012 on COM(2012) 11, Resolution of the Czech Senate on the New Framework for Data Protection, May, 22, 2014, Motion approved by the Plenary of the German Bundestag on the proposal for a General Data Protection Regulation of 13 Dec. 2012, Questions about the General Data Protection Regulation and about the specific Personal Data Protection Directive in Criminal Matters by the Dutch Senate of the States General of May 15, 2012, Letter of the Romanian Parliament on the General Data Protection Regulation of Apr. 3, 2012, Position of the Committee on EU Affairs of the Republic of Slovenia on the proposed General Data Protection Regulation of March 20, 2012.

[179] For example, the Belgian House of Representatives objected to the proposal on subsidiarity grounds but was of the opinion that some matters (mostly those originating in the private sector, and those concerning the exchange of data with non-EU countries) could be left to regulation, whereas data privacy in the public domain had to be dealt with by a directive, so that strict Belgian standards of data protection in the healthcare and social security sectors could be preserved. Belgian Chambre des Représentants, Reasoned

statement, which, unlike the reasoned opinion of the Bundestrat, did not raise subsidiarity objections. Although the Bundestag emphasized the need to disentangle private from public sector data privacy matters to preserve the high standards of protection in Germany, it also held that:

> The lack of harmonization in the (non-public) sphere of the economy results in distortions to competition in the internal market and allows enterprises to deliberately select their location according to the most favourable regulations and enforcement environment (forum shopping). Greater harmonization in the non-public sector would therefore not only lead to greater clarity and fairer competition at the European level, it is also a precondition for European data protection standards being more able to assert themselves in competition with providers from third countries. The German Bundestag underscores that German data protection legislation alone will not be able to provide effective protection against companies acting out of third countries and welcomes the proposal's applicability towards providers in third countries.[180]

Similarly, in its reasoned opinion, the Swedish Parliament (Riksdag) objected to the choice of a regulation on grounds of proportionality, which Parliament believed to be part of the subsidiarity test. Nonetheless, the Riksdag submitted that the objective of an effective system for the protection of personal data in the EU was generally better achieved when measures were undertaken at Union level rather than by the Member States, since due to its scope and effects, EU legislation would in general be "clearly advantageous" compared to a measure at national level.[181] Importantly, through the legislative process, the EP tried to put flesh on the bones of what may be called as high-level demands voiced by the national legislatures. First, most likely in response to

---

opinion of Apr. 6, 2012 on COM (2012) 11, (Rapport fait au nom de la Commission de la Justice, DOC 53 2145/001).

[180] Motion approved by the Plenary of the German Bundestag on the proposal for a General Data Protection Regulation of Dec. 13, 2012.

[181] The Slovenian Parliament, albeit through a statement that did not question compliance with subsidiarity, expressed similar doubts on the choice of a regulation but simultaneously welcomed "the important and useful solutions" offered in the draft, including, among others those regarding human rights protection, data breach notifications, data protection by default, obligatory impact assessments and the "right to be forgotten". Position of the Committee on EU Affairs of the Republic of Slovenia on the proposed General Data Protection Regulation of Mar. 20, 2012.

concerns about pre-existing higher national standards in the public sector voiced by the German, Belgian and French legislatures, the European Parliament proposed an amendment that extended the application of general principles of data protection not only to the employment sector as suggested by the Commission, but also to the social security context. The amended text specified that the regulation purported to establish EU law floors, not ceilings, in these domains.[182]. In addition, the Commission specified in its reply letter to the national parliament that the Proposal does not in any event intend to challenge the decisions of the national data protection authorities, for instance on the use of national identification numbers or in the social security sector.[183]

Second, the EP was responsive to demands that a high level of protection be guaranteed in international data transfers, something that both the Belgian House of Representatives and the German Bundestag insisted on.[184] It further elaborated on measures intended to compensate for the lack of protection in a third country pending an adequacy decision, by stipulating that any such measures like binding corporate rules, standard data protection clauses or contractual clauses should respect the data subject rights valid in intra-EU processing. In particular, the principles of purpose limitation, right to access, rectification, erasure and the possibility to claim compensation were defended in the EP amendments. Additionally, the MEPs suggested that in the absence of an adequacy decision, the principles of data protection by design and by default need to be observed and that guarantees for the existence of data protection officers needed to be provided. The aim was to ensure that legally binding guarantees would be in place so that measures intended to replace the adequacy standard would not effectively subvert EU standards.[185]

---

[182] The amendment uses the language of "minimum standards", European Parliament Legislative Resolution of Mar. 12, 2014 on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to their Personal Data and on the Free Movement of Such Data, amend. 124, COM (2012) 11 final (Jan. 25, 2012).

[183] Commission Reply to the Reasoned Opinion of the Belgian House of Representatives and Commission Reply of Jan. 10, 2013 to the Reasoned Opinion of the German Bundesrat on COM (2012)11.

[184] The EP amended the Preamble of the Regulation to read: "any legislation which provides for extra-territorial access to personal data processed in the Union without authorization under Union or Member State law should be considered as an indication of a lack of adequacy", *see infra* note 182, amend. 55.

[185] Ultimately, Parliament insisted that financial indemnification be available in cases of loss or unauthorized processing or access to the data and that regardless of national legislation, the entity in the third country would have an obligation to provide full details of all access to the data by public authorities. EP also suggested amendments to the Regulation asking the Commission to ensure that Union law takes

Finally, in accordance with the demands of the majority of national parliaments, EP proposed amendments that would drastically limit the Commission's powers to adopt implementing and delegated acts.[186] The Commission explained the provisions as motivated by a desire to provide a general legislative framework on data protection while leaving some of the details to be specified at a later stage to avoid rigidity and ossification.[187] The EP proposed that in the remaining areas of delegation, the Commission consult the European Data Protection Board, for instance on the right to be forgotten and erasure; on deciding the validity of codes of conduct; when specifying criteria on certification mechanisms and when deciding on adequacy standards in third countries, territories, processing sectors or international organizations.[188] Under the EP amendments, the Data Protection Board would be authorized to issue opinions on the lead supervisory authority at the request of any of the national competent authorities.[189]. In cases of cross-border EU data exchange that affects individuals in more than one state, the lead supervisory authority (normally defined as the DPA of the country where the business is established) would collaborate with other concerned national DPAs to reach a final agreement on a consumer's complaint, with the European Data Protection Board serving as a dispute settlement mechanism.[190]

---

precedence at all times when controllers or processors are confronted with conflicting compliance requirements under EU law and the jurisdiction of a third country, and that no judgment of a court or tribunal and no decision of an administrative authority of a third country requiring disclosure of personal data is recognized or enforceable in any manner, *see infra* note 182, amend. 62-63.

[186] Under the amendment, the Commission would be stripped of such powers regarding the "...lawfulness of processing; specifying the criteria and conditions in relation to the consent of a child; processing of special categories of data; specifying the criteria and conditions for manifestly excessive requests and fees for exercising the rights of the data subject; criteria and requirements for the information to the data subject and in relation to the right of access; measures based on profiling; criteria and requirements in relation to the responsibility of the controller and to data protection by design and by default; criteria and requirements for the documentation and the security of processing; criteria and requirements for establishing a personal data breach and for its notification to the supervisory authority, and on the circumstances where a personal data breach is likely to adversely affect the data subject; the criteria and conditions for processing operations requiring a data protection impact assessment; the criteria and requirements for determining a high degree of specific risks which require prior consultation; designation and tasks of the data protection officer...transfer derogations...[and]... processing for historical, statistical and scientific research purposes...", *see infra* note 182, amend. 91.

[187] Commission Reply of Feb. 21, 2013 to the reasoned opinion of the Italian Camera dei Deputati on COM (2012) 11.

[188] *See infra* note 182, amend. 158.

[189] Questions about the General Data Protection Regulation and about the specific Personal Data Protection Directive in Criminal Matters by the Dutch Senate of the States General of May 15, 2012 (The EP thus answered a query posed by the Dutch Parliament).

[190] The success of this strategy would likely depend on the viability of the European Data Protection Board to function as an effective venue of horizontal coordination between the data protection authorities.

By partly outsourcing the specifics to the European Data Protection Board and leaving regulatory details to be clarified later by the coordinated effort of national data protection authorities, the EP aimed to accomplish the objective of keeping pace with innovation while avoiding over-centralization. Although it is difficult to establish a direct link between the course of action that the EP chose to take and the demands of the national legislatures, it is evident that some of the most prominent concerns of the national legislatures found their way into the European legislative process.[191]

5. The Role of the National Highest Courts in the EU

In no small measure, the national constitutional courts of the EU Member States play the role of watchdogs over EU data protection centralization in law enforcement. Several of the EU Member States' constitutional courts have prepared the groundwork for the landmark ECJ judgment invalidating the EU Data Retention Directive.

The influence of the German Federal Constitutional Court (Bundesverfassungsgericht, hereafter BVerfG) on ECJ's reasoning is noteworthy. However, the leading role of German privacy law in the EU has not remained uncontested. Following 9/11 and the terrorist attacks in the London subway in 2005, several Member States within the EU unilaterally adopted specific legislation providing for the retention of data by service providers. In 2006, the EU passed the Data Retention Directive, aimed at facilitating the Member States' fight against terrorism and serious crime through the retention of telecommunications data (known also as *traffic* or *meta* data as opposed to *content* data). The background of the Directive's enactment in the aftermath of the Madrid train bombings points to a coalition between the UK, French, Swedish and Irish governments that originally suggested a legislative act which would

See Council Position on the 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, 9565/15 (June 11, 2015), paras. 97-106. The Commission version of the Regulation has established a "one-stop shop" (consistency mechanism), based on the EU principle of mutual recognition that permeates many other areas of EU law. The basic idea behind this principle is that goods or services lawfully marketed in one Member State should be allowed at the market of another Member State even if they do not fully comply with the technical rules of the Member State of destination. Given possible divergences between the DPAs of the Member States when they interpret EU data protection law, horizontal coordination between them seems both promising and a necessary supplement to the "one-stop shop" mechanism.

[191] Neither the EP nor Council versions are final. The proposed Regulation is subject to the completion of the ordinary legislative procedure. For a summary, *see* PAUL CRAIG & GRÁINNE DE BÚRCA, EU LAW: TEXT, CASES, AND MATERIALS 123-129 (5th ed. Oxford Univ. Press, 2011).

have been closer to the subject matter of the Directive but would have at the time limited the involvement of the European Parliament in the legislative process.[192] In addition, the original text of the proposal proposed retention periods between 12 and 36 months. In the face of multiple criticisms on various counts, the final text of the Data Retention Directive was couched on a market harmonization legal basis. It provided for storage of no less than six months and no more than two years of all citizens and legal entities' traffic and location data necessary to identify the subscriber or registered user of all types of telecommunications. In order not to stir controversies over whether the EU had competence to act in the criminal law field, the Directive excluded a uniform definition of what constituted a "serious crime", but required the retention and prompt exchange of traffic data for law enforcement purposes. Instead, the Directive left it to Member States to decide what was "serious crime" and a trigger the Directive's application.

The Commission's evaluation report on the implementation of the Data Retention Directive showed that at least ten Member States have taken the opportunity to impose requirements stricter than those espoused in the Directive, for example by transposing into their national legislation a "serious crime" to mean a minimum prison sentence or even a custodial sentence.[193] Eight Member States have gone further by requiring data to be retained not only for investigation, detection and prosecution in relation to serious crime, as mandated by the Directive, but also for all criminal offences, crime prevention and public security in general[194] while four Member States left out the definition of a "serious crime" altogether,[195] leaving space for arbitrary interpretation. Generally, the EU Member States have faced difficulties in implementing the Data Retention Directive, which was strongly opposed by civil society actors.[196] Eventually, various procedures

[192] Draft Framework Decision on the Retention of Data Processed and Stored in Connection with the Provision of Publicly Available Electronic Communications Services or Data on Public Communications Networks for the Purpose of Prevention, Investigation, Detection and Prosecution of Crime and Criminal Offences Including Terrorism, Council Doc 8958/04 (Apr 28, 2004).

[193] These were Bulgaria, Estonia, Ireland, Greece, Spain, Lithuania, Luxembourg, Hungary, the Netherlands, and Finland. Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC) COM(2011) 225 final, Apr. 18, 2011.

[194] Belgium, Denmark, France, Italy, Latvia, Poland, Slovakia, and Slovenia, *id*.

[195] Cyprus, Malta, Portugal, and United Kingdom, *id*.

[196] In 2007, two months after the Data Retention law was approved in Germany, a newly formed privacy NGO called 'Arbeitskreis Vorratsdatenspeicherung' (Working Group on Data Retention) filed a formal constitutional complaint with the German Federal Constitutional Court by an unprecedented 34,000 complainants. From 2006 to 2009 the same group organized ten peaceful demonstrations in cities

claiming the unconstitutionality of the national transposition acts were introduced before domestic high courts. The Bulgarian Supreme Administrative Court, the Czech Constitutional Court, the Cypriot Supreme Court, the BVerfG, and on two occasions – the Romanian Constitutional Court all found the respective national implementing acts (or parts thereof) void under the national constitutions. In addition, the Austrian Constitutional Court sent a preliminary reference to the ECJ about the interpretation of the Data Retention Directive while the Slovenian Constitutional Court decided to suspend its decision until the ECJ decided on the validity of the Directive in the *Digital Rights Ireland*[197] case.

In *Digital Rights Ireland,* the ECJ eventually invalidated the Directive in its entirety and with immediate effect. The *ratio dicidendi* of the ECJ's decision resembled that of the national courts, and included much of the reasoning[198] that preceded it, but is arguably most similar to the BVerfG's argumentation. The national courts' reasoning bears similarities also horizontally: specifically, the German and the Czech Constitutional Courts. Both courts invalidated the domestic acts implementing the Directive on proportionality grounds, and placed emphasis on transparency, citing as a major drawback of the domestic laws the fact that the persons concerned would not be aware their data had been requested.[199]

The reasoning of the BVerfG (and in turn, the ECJ) revolved around three main arguments: first, both courts denounced the chilling effect of indiscriminate surveillance

---

across Germany with participation numbering in the several hundred thousands. Partners in such initiatives were also the Brussels-based NGO 'European Digital Rights', the US-based 'Electronic Privacy Information Center' (EPIC) and the anti-surveillance Madrid-based 'Destapa el Control' (Take the Lid Off). Christian DeSimone, *Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive*, 11 German L. J. 291, 307 (2010).

[197] Case C-293/12 and Case C-594/12, Digital Rights Ireland Ltd. v Minister for Communications, Marine and Natural Resources & Kärntner Landesregierung and Others, 2014, E.C.L.I. 2014: 238.

[198] Franziska Boehm and Mark De Cole, *Data Retention after the Judgment of the Court of Justice of the European Union*, Report for the Greens: European Free Alliance in the European Parliament, (2014) at: http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf. Unlike the Romanian Court, however, the ECJ did not declare that the very core of the right to privacy is affected, *id*.

[199] The German Federal Constitutional Court (Bundesverfassungsgericht, BVerfG) explained that secret processing is only to be permitted when the specific case requires it, in which case a court order is still needed, and notification of processing must be made after the fact. *See* Eleni Kosta, *The Way to Luxembourg: National Court Decisions on the Compatibility of the Data Detention Directive with the Rights to Privacy and Data Protection*, 10 SCRIPTED (2013) (discussing the national court decisions).

on the exercise of fundamental rights;[200] second, both courts emphasized the danger of profiling, which blurs the line between meta- and content data,[201] and third, both courts found that the undifferentiated character of long data retention periods coupled with insufficiently restrained access to the data[202] (thereby contravening the FIPP of purpose limitation) did not meet the proportionality test. Ultimately, some would like to know: wouldn't the ECJ invalidate the Directive even if it weren't for the national courts decisions? After all, the European legal system, based on shared principles of balancing privacy with other rights and interests, first established under German law, is not at all that different from those of its constituent countries. Even despite the fact that the ECJ

[200] The BVerfG held that mass data retention produces the "diffusely threatening feeling of being watched", *see* Christian DeSimone *supra note* 196. Similarly, the ECJ found that retained data subsequently used without the knowledge of the data subject is "likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance", *see supra* note 196 at para. 37.

[201] The ECJ held that: "Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.", see *supra* note 197, at para. 27. The BVerfG similarly noted that traffic data is hardly distinguishable from content date, since the recipients, dates, time and place of telephone conversations, if they are observed over a long period of time, permitted detailed information to be obtained on social or political affiliations and on personal preferences, inclinations and weaknesses. Since profiling increased the risk of citizens being exposed to further investigations without having given occasion for it and also exposed to risk in particular certain professions such as journalism, hot lines, medicine, politics and the law, the German court found that the burden on fundamental rights is no less severe in the case of traffic data profiling, *See supra* note 197.

[202] The BVerfG assessed as disproportional the blanket retention of data, since such retention did not refer to the factual circumstances of a case where the authorities must suspect with sufficient probability that someone has committed a concrete crime of considerable weight before their data are retained and processed. Thus, the German law would convert virtually all German citizens into potential criminal suspects. In addition, the BVerfG found the transposition of a "serious crime" into German law that required access to be given to law enforcement officials "if facts justify the suspicion that someone has committed a crime of considerable seriousness or a crime using telecommunications" to be so loose that any fact-based suspicion of a non-petty crime could meet the threshold. The ruling criticized the expansion of prosecutorial purposes to any crime "using telecommunications" as trivializing the intended exceptional nature of data processing. Katja de Vries, Rocco Bellanova, Paul De Hert, and Serge Gutwirth, *The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't It?), in* COMPUTERS, PRIVACY AND DATA PROTECTION: AN ELEMENT OF CHOICE 12 (SERGE GUTWIRTH, YVES POULLET, PAUL DE HERT & RONALD LEENES, EDS., SPRINGER, 20122). The ECJ in turn characterized the Directive as covering, "...in a generalized manner all persons and all means of electronic communication, as well as all traffic data without any differentiation, limitation or exception being made in light of the objective against serious crime." The ECJ's rationale was that the Directive was overly broad, in that it applied even to persons for whom there was no evidence that "their conduct might have a link, even an indirect or remote one, with serious crime." *See supra* note 197, paras. 57-58. Regarding the definition of "serious crime", the ECJ also found that the Directive "...fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use", *id*. at para. 60.

upheld the Directive under an earlier challenge on the legal basis,[203] it likely could have invalidated it when it reached the question of fundamental rights in *Digital Rights Ireland*. However, it should also be borne in mind that the shared proportionality framework allows the national courts and the ECJ to have a common but flexible "toolkit," one that is not necessarily bound to results. It is indeed that open-ended character of proportionality that has led to its increased uptake in European public law adjudication.[204] As a consequence , with respect to privacy, as well as in other fields, the proportionality test does not exclude future rebalancing of rights and interests. The "nudging" effect that the Member State courts had on the ECJ was therefore significant for the outcome of *Digital Rights Ireland*.

Built around a robust set of the FIPPs on which many EU member states have now converged, the model of data protection defended by the domestic constitutional courts and the ECJ in the data retention cases is based on providing strong safeguards when infringements to data privacy are deemed strictly necessary for the public interest. However, further challenges to centralizing data protection on the EU level based on such a model are expected to come in the wake of national legislation that permits intelligence services to collect metadata in real time without any judicial oversight, as, for example, in the UK,[205] and the approval of intrusive anti-terrorism measures, as in France, in the aftermath of the Charlie Hebdo terrorist attack.[206]

CONCLUDING REMARKS

Data privacy policies and lawmaking in the US and the EU function in a federated fashion and form part of the broader tussles surrounding the allocation of powers

[203] Case C-301/06 Ireland v. Parliament and Council, E.C.L.I. 2009:68, 2009.

[204] Alec Stone Sweet & Jud Matthews, *Proportionality Balancing and Global Constitutionalism*, 47 COLUM. J. TRANSNAT'L L. (2008).

[205] Triggered by the *Digital Rights Ireland* case, the overhaul of bulk data collection by the UK's Government Communications Headquarters (GCHQ) is still under way. As remarked by UK's Independent Reviewer of Terrorism Legislation, in not having any prior judicial authorization mechanism for the interception of communications, the UK is an outlier even amongst the so-called Five-Eyes States (the US, Australia, New Zealand, Canada and the UK) that share intelligence. *See* DAVID ANDERSON, A QUESTION OF TRUST: REPORT OF THE INVESTIGATORY POWERS REVIEW at 349 (2015).

[206] *See supra* note 65. *See* also Aurelien Breeden, *France Clears Final Hurdle to Expand Spying Power*, N.Y. TIMES, JULY 25, 2015, at A8.

between the federal and the state tier. However, in both contexts the intersection of privacy and federalism has yet to be sufficiently studied, and the risk of ossification and over-centralization of data privacy solutions tends to be overstated.

I have here argued for the benefits of degree of autonomy in a web of interconnected federal and EU data privacy sites. Autonomy needs to be protected, because it gives states and localities the ability to defy the policy *status quo* by developing specific innovative solutions to balance fundamental rights (or consumer rights) with other rights and interests. When enabled to act in this way, the states become "disaggregated sites of national [or EU] governance,"[207] channeling legislation on issues of major concern to the American people or to EU citizens before the federal or the EU legislature can step in. When hammering out a more manageable judicial approach to the privacy safeguards of federalism both in the US and in the EU, the preemption doctrine needs further specification across a temporal dimension. States can be given sufficient space to experiment with privacy regimes because state entrepreneurship (such as in the case of German data protection law, or the emerging Californian model in the US) provides policy expertise to the federal or the EU legislature. It offers windows of opportunity for centralizing data privacy around a relatively high bar. This is especially significant, given that technology facilitates spillover effects across state jurisdictions, and since private companies tend to adapt to the higher standard of protection, which often become engrained into their corporate business models. Finally, as one interviewee shared:

> Of course, [in the US] business entities look mostly at New York, Florida, California and Massachusetts the same way as Germany, Spain, UK and France are setting the tone in Europe. But even if a small state adopted a law, the industries would have to comply instead of risking enforcement costs; no one wants his or her picture in the newspaper when an attorney general starts an investigation. Nobody wants to be prosecuted, even in South Dakota.[208]

[207] *See supra* Jessica Bulman-Pozen at note 31.
[208] *See supra* note 78.

Ultimately, the "presumption against preemption" can be stronger, at least until the baton gets passed to a federal or the EU lawmaker. A more case-by-case approach might be carved out after that.

Taken as a case study, privacy has a lesson or two for federalism theory, too. Instead of waiting for Godot by hoping to insolate areas of impenetrable state domination—usually by looking for judicial bright lines, or engaging with the idea of channeling precious state power (usually through politics)—the concept of federalism's safeguards needs to be rethought.[209] The safeguards of privacy federalism are both political *and* judicial. Both judicial and political institutions (including the state institutions) have a role to play in building well-functioning democracies. The national parliaments and the data protection authorities are able to voice regional concerns in the EU. Similarly, the national legislatures and state attorneys general in coordination with federal agencies in the US maintain the democratic character of privacy consolidation at the US federal level. Further, in accordance with the EU and the US dual systems of judicial protection, the highest domestic courts are able to police fundamental rights under their national constitutions and can also offer a springboard for the reinterpretation of EU or US federal law. After a period of horizontal experimentation has passed, it might be to the benefit of individuals, businesses and law enforcement alike to adopt harmonized measures and reduce complexity. Or, at least until a new cycle of policy change begins.

[209]Cf. California's waiver under the Clean Air Act to regulate vehicle emissions beyond the floor set by the Environmental Protection Agency (EPA). "The EPA began with national uniform standards and moved to the proposal for the more stringent [Californian standard] only after a movement began in the states toward adopting the most stringent Cal LEV standards", *see* Kirsten H. Engel *supra* note 56 at 171-2.

NYU School of Law • New York, NY 10011