Center for European Studies Working Paper Series #174 (2010)

The Non-Americanization of European Regulatory Styles: Data Privacy Regulation in France, Germany, Italy, and Britain

Francesca Bignami

Professor of Law
George Washington University
2000 H Street, N.W.
Washington, DC 20052
Email: fbignami@law.gwu.edu

Abstract

European countries have experienced massive structural transformation over the past twenty-five years with the privatization of state-owned industries, the liberalization of markets, and the rise of the European Union. According to one prominent line of analysis, these changes have led to the Americanization of European regulatory styles: previously informal and cooperative modes of regulation are becoming adversarial and litigation-driven, similar to the American system. This article explores the Americanization hypothesis with a structured comparison of data privacy regulation in four countries (France, Britain, Germany, and Italy) and a review of three other policy areas. It finds that European regulatory systems are converging, but not on American-style litigation, rather on an administrative model of deterrence-oriented regulatory enforcement and industry self-regulation. The explanation for this emerging regulatory strategy is to be found in government responses to market liberalization, as well as the pressure created by the governance process of the European Union.

THE NON-AMERICANIZATION OF EUROPEAN REGULATORY STYLES: DATA PRIVACY REGULATION IN FRANCE, GERMANY, ITALY, AND BRITAIN

Table of Contents

I. Introduction

One of the defining characteristics of a nation is its regulatory style.[1] The concept of regulatory style refers to the complex legal and political process through which government regulators, the public, and the business community interact to make and implement public policy. In the 1970s and 1980s, regulatory styles varied considerably among nations: informal and cooperative in Great Britain, hierarchical and rule-oriented in France, and punitive and litigious in the United States, what has been dubbed by Robert Kagan as the distinctive American style of "adversarial legalism."[2] Today, however, with the privatization and liberalization of European markets, the spread of New Public Management regulatory tools, and the rise of the European Union, a number of scholars argue that Europe is coming to resemble America. In other words, the distinctively American system of transparent and adversarial administrative proceedings,

[1] Professor, George Washington University Law School.

I would like to thank Maria Teresa Annecca, Sue Chen, Claudia Haupt, Dana Jenztsch, Florence Kramer, Clea LeThuc, Karen Linhart, Elizabeth Morrow, Mariana Tavarres, and Myron York for their excellent research assistance. I would also like to thank participants in workshops held at Duke Law School, the University of Wisconsin-Madison, and the Center for European Studies at Harvard University for their suggestions on different versions of this project. I am grateful to Robert Keohane for his comments on the project at its early stages and to the German Marshall Fund for providing the financial support for my fieldwork.

[2] *See* ROBERT A. KAGAN, ADVERSARIAL LEGALISM 3 (2001); DAVID VOGEL, NATIONAL STYLES OF REGULATION 269-70 (1986); Jack Hayward, *Mobilising Private Interests in the Service of Public Ambitions*, in POLICY STYLES IN WESTERN EUROPE 114 (Jeremy Richardson ed., 1982).

punitive administrative enforcement and, most importantly, pervasive regulatory litigation is being copied in Britain, France, Germany, and the rest of Europe.[3]

This article seeks to assess the Americanization claim and to contribute to our understanding of the nature and the origins of regulatory change in Europe. It does so with empirical data from a structured comparison of one policy area—data privacy—in four European countries (France, Britain, Germany, and Italy) and with supporting evidence from three other policy areas. The main finding is that European regulatory styles are converging, but not on a system of adversarial legalism, as expected in the Americanization literature, rather on a regulatory process that combines tough, legalistic administrative enforcement of government rules with extensive public pressure on industry actors to self-regulate.

To understand the causes of this pattern of convergence, I draw on but also significantly rework the theory of one of the main proponents of Americanization, Daniel Kelemen.[4] Kelemen points to market liberalization and the federalization of political power (generally known as Europeanization) as the main causes of change and, indeed, I find that both forces have put pressure on national policymakers to alter their traditional approaches to privacy regulation. However, the type of convergence that I identify is largely unanticipated by Americanization theory and this is so because the theory both fails to adequately unpack the concept of regulatory style and gives only a partial account of the process of Europeanization. A regulatory style has three dimensions—the institutions charged with policy implementation, the administrative procedures used by bureaucrats, and the regulatory instruments used to accomplish public purposes. The institutional dimension—whether administrative agencies alone, as in Europe, or courts and administrative agencies together, as in the United States, are entrusted with implementation—has proven to be far more resistant to change than the other two because of the highly path-dependent nature of national courts and legal doctrine. Therefore, although the European Commission has succeeded in pushing national administrative agencies to adopt a more legalistic approach to regulatory enforcement, it has not been able to enlist national courts in the regulatory process. Furthermore, Kelemen's account of Europeanization focuses exclusively on the vertical pressure exerted by EU institutions on national governments. Yet, as my analysis shows, Europeanization also facilitates horizontal policy diffusion among member states. Through this diffusion process, self-regulation, which was once only popular in traditionally cooperative and flexible regulatory systems like Britain and Germany, has taken hold in countries like France and Italy with a reputation for being hostile to industry participation in policymaking.

The rest of this article proceeds as follows. The first part explains the concept of national regulatory styles, reviews the theory of Americanization of European regulatory styles, and develops an alternative approach based on the findings presented in the empirical sections of the article. The second part explains the rationale for my selection

[3] R. Daniel Kelemen, *Suing for Europe*, 39 COMP. POL. STUD. 101 (2006).
[4] *Id*.

of the policy case and the country cases and reviews the empirical methods that I used in the study.

The third part analyzes privacy regulation in those countries with early data privacy laws—France, Germany, and Britain—and exposes their distinctive regulatory styles. Data privacy was first regulated by European countries in the 1970s, in response to the development of new computer technologies and the vast quantities of personal data that suddenly became available to governments and corporate actors. I show that these early privacy systems displayed the distinctive attributes of their overarching national regulatory styles that have been identified in the comparative public policy literature. The British system was the most informal and cooperative, relying heavily on self-regulation and informal dispute settlement, the French one was the most hierarchical, with significant licensing and rulemaking powers exercised by government regulators, and the German one stood close to the British one. In none of these systems, in contrast with the American regulatory style, was litigation a significant force.

In the fourth part, I examine how the two major transformations that have occurred since the 1970s—the digital revolution and the Europeanization of privacy policy—have put pressure on national policymakers to alter their traditional approaches to privacy regulation. The digital revolution and the resulting proliferation of market actors covered by privacy regulation have forced regulators to cut back on flexible but resource-intensive licensing and registration. This same proliferation of market actors has made deterrence-oriented regulatory enforcement and self-regulation attractive to overwhelmed government bureaucrats. But even though these regulatory strategies might be appealing, their adoption across a widely disparate set of national contexts has been driven by Europeanization. With the EU Privacy Directive, passed in 1995, southern countries have come to rely on self-regulatory techniques championed by northern countries and administrative agencies everywhere have come under pressure to pursue a legalistic approach to enforcement.

The fifth part examines contemporary national systems, which, with the passage of the first Italian privacy legislation in 1996, also include Italy. It unpacks the political and legal process through which national systems have converged on a dual strategy of self-regulation and legalistic administrative enforcement and demonstrates that litigation remains an insignificant component of the regulatory scheme in all countries. In the sixth part, I review developments in anti-discrimination law, environmental policy, and consumer protection, to suggest that this pattern of regulatory change marks not only the privacy arena but also a wide range of other European policy areas. The conclusion summarizes the main points of the study and explores the implications for comparative law research on convergence and legal transplants.

II. Theoretical Framework

How public policy gets implemented in democratic societies turns on a number of interrelated factors. Comparative research from the 1970s and the 1980s focused on variations on three important dimensions of the regulatory process: institutions,

procedures, and instruments. European countries and the United States were found to differ on each of these dimensions.[5] The *institutions* charged with implementation could be almost exclusively state bureaucracies, as in Europe, or could be courts and bureaucracies, as in the United States. The *administrative procedures* used by bureaucrats to formulate policy could be informal and opaque, as in Europe, or law-governed and transparent as in the United States. And the *regulatory instruments* used to implement policy goals could be open-ended, flexible, and managerial as in most of Europe, or precise, rigid, and punitive as in the United States. Taken together, these features of the American process—what Robert Kagan calls "adversarial legalism"—meant that regulators had little policymaking discretion and were embedded in an adversarial set of relations with the business community and the public. By contrast, in Europe, bureaucrats had great policymaking freedom and relations between administration and industry were cooperative and consensual.

Notwithstanding the marked contrast between Europe and the United States, variations also existed within Europe.[6] First, in some systems (Britain, Germany, the Netherlands) the administrative process was fairly open to organized interests, involving informal consultation and official committees of interest group representatives, while in other countries (France) policy was determined by bureaucratic elites operating in relative freedom from organized interests. Second, this openness to organized interests in Britain, Germany, and elsewhere corresponded with a greater reliance on self-regulatory instruments—the allocation of authority to industry groups to elaborate and enforce standards of corporate conduct. Third, regulatory standards were especially flexible in Britain and more precise and legally binding in continental European systems. The chart below summarizes these transatlantic and European differences in regulatory styles.

	United States	**European Systems**	
Institutions	Courts and bureaucracy	Bureaucracy	
Administrative Procedure	Transparent and formal	Informal consultation and official interest group committees	Closed to interest groups
Policy Instruments	Detailed rules and deterrence-oriented enforcement	Vague standards and self-regulation	Binding legal standards and little self-regulation

Today, however, scholars argue that European systems are converging on a regulatory process that closely resembles the American one: litigation-driven,

[5] *See* Robert A. Kagan, *Should Europe Worry About Adversarial Legalism?*, 17 OXFORD J. OF LEGAL STUD. 165 (1997).
[6] *See* DAVID VOGEL, NATIONAL STYLES OF REGULATION 269-70 (1986); POLICY STYLES IN WESTERN EUROPE 18, 169, 114 (Jeremy Richardson ed., 1982).

transparent, and legalistic.[7] Daniel Kelemen, one of the main proponents of this view, identifies two major causal factors that are pushing European policy styles towards this Americanized model, one having to do with the organization of markets and the other related to the governance structure of the European Union. According to his theory, the liberalization and re-regulation of markets that occurred in the 1980s and 1990s has given rise to detailed rules, by-the-book enforcement, transparent agency procedures, and active courts, inevitably drawn in to police all of these law-bound interactions. Kelemen also argues that adversarial legalism is being driven by the extreme fragmentation of government authority in the European Union, where legislative power is exercised at the center but executive power rests with the member states. This argument draws on rational choice accounts of policymaking in political science and turns on the difficulty of enforcing policy bargains in a universe of divided executive and legislative power.[8] In this line of analysis, credible commitments—detailed rules, litigation rights, independent courts and regulatory agencies, and sanctions—are the answer to the bargain-enforcement problem. According to Kelemen, these credible commitments are being written into EU law and are empowering courts and litigants in the domestic regulatory process.

This model is a useful starting point for understanding regulatory convergence in Europe. As I demonstrate in the empirical section, both the re-organization of markets and the logic of credible commitments have driven convergence in my cases. The proliferation of market actors has pushed data privacy regulators away from flexible, but resource-intensive, policy instruments like case-by-case licensing and towards a greater emphasis on punishing for rule violations. In a wide array of policy areas, the European Commission has insisted that domestic regulators be given tough enforcement powers and independence from their governments to ensure that EU policy bargains will be faithfully executed at the member-state level. However, in important respects, the type of convergence that I find departs from the adversarial legalism hypothesis. At least in the privacy field, there has been little pressure to change administrative procedure. Contrary to the rigid, precise form of regulation anticipated by the Americanization hypothesis, self-regulation is on the rise across a broad spectrum of policy areas. Furthermore, litigation has not emerged as a significant component of the regulatory process. The chart below summarizes the differences between the convergence anticipated by Americanization theory and the findings from my empirical study.

---

[7] *See* Kelemen, *Suing for Europe*, supra note 3; Colin Scott, *Privatization and Regulatory Regimes*, in THE OXFORD HANDBOOK OF PUBLIC POLICY 651 (Michael Moran et al. eds., 2006); Mark Thatcher, *Analysing Regulatory Reform in Europe*, 9 J. EUR. PUB. POL'Y 859 (2002).

[8] *See, e.g.*, GEOFFREY GARRETT, THE POLITICS OF LEGAL INTEGRATION IN THE EUROPEAN UNION, 49 INTERNATIONAL ORGANIZATION 171 (1995) (European Union), DAVID EPSTEIN & SHARYN O'HALLORAN, DELEGATING POWERS (1999) (American politics) ; Robert O. Keohane, *Institutional Theory and the Realist Challenge After the Cold War* in NEOREALISM & NEOLIBERALISM 269 (David A. Baldwin ed., 1993) (international relations).

	Hypothesized Regulatory Style	Actual Regulatory Style	
Institutions	Courts and bureaucracy	Bureaucracy	
Administrative Procedure	Transparent and formal	Informal consultation and official interest group committees	Closed to interest groups
Policy Instruments	Detailed rules and deterrence-oriented enforcement	Deterrence-oriented enforcement and self-regulation	

The paucity of litigation is one of the biggest problems for Americanization theory. In the privacy case, as well as the other policy areas that I take up at the end of the article, there have been various attempts to improve litigant rights, but they have consistently been beaten back by skeptical governments and legal scholars. Moreover, in the law-in-action, litigation has not had an impact. In my study, in no national system do privacy regulators report being taken to court more often now than in the past. Furthermore, the data set that I constructed on statutory tort cases brought by privacy victims between 1980 and 2007 did not show an increase in litigation rates. Litigation in Italy, Germany, and France was low and constant, and damages awards were modest. (Indeed in Germany they were never awarded.) Britain is a partial exception in that litigation did rise slightly, but in no way can it be said to be a significant component of the regulatory scheme: the numbers went from virtually no litigation in the 1980s and 1990s to an average of three to four cases decided per year by the main trial court in the 2000s.

Neither is the data presented by Kelemen adequate to support the Americanization hypothesis. He offers impressive aggregate-level figures on growth in the number of lawyers in Europe, the increasing market value of the legal services industry, and other indicators, but he does not have data on trends in litigation rates or damages awards. Although it is true that courts can influence markets and regulators through simply the risk of litigation, we would still expect evidence of an increased perception of risk. Without more, rising numbers of lawyers and growing expenditures on legal services do not tell us much about this risk. In increasingly complex societies, in which more and more behavior is governed by legal rules, we would expect both government administration and business to rely heavily on legal counsel to understand what is required of them under the law. Whether those lawyers are spending more time than before in court, defending their clients in high-stakes litigation, or threatening to take others to court is a different matter. What is needed to convincingly make the case for adversarial legalism and what still does not exist are data showing increases in litigation rates, damages awards, public reports of punitive damages, and other indicators to suggest that fear of the courtroom looms larger than before in both the government and corporate worlds.

How can we explain the failure of litigants and courts to emerge as significant players in the European regulatory process? The answer to this puzzle lies in the path-dependent nature of courts and the interconnected system of legal rules, judicial decisions, academic scholarship, and legal education that constitutes any legal order.[9] To use the schema outlined earlier, it is far more difficult to change the institutions involved in the policymaking process and to insert courts as equals to bureaucrats, than it is to simply convince bureaucrats to switch regulatory tools and punish more. It is impossible to do justice in this brief section to the complex reasons for this pattern of European resistance to change, but the key is to be found in the difference between law conceived as a free-standing, technical discipline and law understood in legal-realist terms, as a malleable instrument designed to accomplish various policy ends. American tort litigation under regulatory statutes, which includes litigation-facilitating devices such as class actions, treble damages, and attorneys fees awards, has been fueled by the legal-realist approach to law: private litigation between two parties can be legitimately used to protect society-at-large and punish for violations of regulatory statutes.[10] Although one must beware of generalizing, in European legal systems, by contrast, tort law is understood as a set of technically complex rules that determines what type of harm gives rise to a legitimate claim for damages.[11] The purpose is to afford a remedy, not deterrence, which is believed to be handled best by the police, administrative authorities, and the "political" branches of criminal and administrative law. These drastically different American and European understandings of the law are embedded in legal doctrine, are perpetuated in legal education, and are repeated and reinforced daily, in the interactions of the legal establishment. No wonder, then, that the numerous attempts of the European Commission to make specific regulatory standards actionable under national tort law have met with protest from national legal elites who fear the contamination of their systems of private law.[12]

The other difficulty with the analytical framework put forward by Kelemen is that it overlooks a critical source of convergence—policy diffusion. As defined by Beth Simmons, Frank Dobbin, and Geoffrey Garrett, "[i]nternational policy diffusion occurs when government policy choices in one country are systematically conditioned by prior policy choices made in other countries (sometimes mediated by the behavior of international organizations or even private actors or organizations)."[13] Policy diffusion has been credited with influencing the timing and geographical scope of economic liberalization, the rise of democratic institutions, and the adoption of constitutions. A number of mechanisms are believed to contribute to diffusion: coercion, competition, learning, and emulation.[14] Within the European Union, the diffusion of policy ideas among national regulators is particularly intense because of the dense set of transnational

[9] *See* Oona Hathaway, *Path Dependence in the Law*, 86 IOWA L. REV. 601 (2000-2001); PAUL PIERSON, POLITICS IN TIME (2004).
[10] Similar reasons are behind European and American differences in administrative law litigation.
[11] *See generally* JOHN HENRY MERRYMAN, THE CIVIL LAW TRADITION (3d ed. 2007).
[12] *See* Reinhard Zimmerman, *Comparative Law and the Europeanization of Private Law*, in THE OXFORD HANDBOOK OF COMPARATIVE LAW 539 (Mathias Reimann & Reinhard Zimmerman eds., 2006).
[13] Beth A. Simmons, Frank Dobbin & Geoffrey Garrett, *Introduction: The International Diffusion of Liberalism*, 60 INT'L ORG. 781, 787 (2006).
[14] *Id.* at 781.

policymaking networks that exist in virtually every area of social and economic governance.

In the privacy arena, as well as the other policy areas that I review, self-regulation has become an increasingly popular technique throughout Europe by virtue of this policy diffusion pathway. I find that privacy regulators from countries like Britain, the Netherlands, and Germany, with extensive experience with self-regulation, have promoted these instruments in EU networks, and that policymakers from countries like France and Italy, without such experiences, have been eager to adopt them. Moreover, regulators in these northern countries have been open to experimentation with new self-regulatory techniques, which differ in important ways from the older ones but which nonetheless still allow for more industry initiative and flexibility than command-and-control regulation. And, again, these instruments have migrated to southern countries via EU networks.

This revised and extended analytical framework offers a better understanding than Americanization theory of the nature and origins of regulatory convergence in contemporary Europe. It breaks down national regulatory styles into institutions, administrative procedures, and regulatory instruments, and shows why the institutional dimension of a regulatory style—the greater or lesser involvement of courts in the policymaking process—is particularly resistant to change. In addition, it identifies policy diffusion and EU networks as a factor that has contributed to regulatory convergence.

III. Case Selection and Methodology

Data privacy was selected as the policy case for exploring changing European regulatory styles for two reasons. First, the independent variables behind the Americanization hypothesis are at work in the data privacy field. Data privacy regulation first emerged in the early 1970s, at a time when the differences in regulatory styles between America and Europe and among European countries were at their peak. Since then, those economic sectors most affected by privacy regulation have been liberalized: banking, financial services, and network industries have all witnessed a shift from public to private ownership, increased competition, and a proliferation of market actors. Moreover, data privacy policy has been Europeanized. In 1995, the European Union entered the policy arena with the Data Privacy Directive, and, as is typical, allocated the executive power of policy implementation to the member states, thus giving rise to the need for credible commitments.[15]

The other reason for selecting data privacy is that previous comparative research on the policy area showed that early national regulatory styles fit with the system-wide, ideal type differences described above and therefore any transformations discovered in regulatory styles could also be expected to be representative of the broader universe of policymaking. In his 1992 book, Colin Bennett demonstrated that the early substantive

[15] Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31.

goals of American and European (British, Swedish, and German) privacy policy were extremely similar, but that the institutions and policy instruments responsible for implementation diverged considerably and differed along the lines anticipated in the comparative public policy literature.[16] My study adds to his account of early regulatory styles by considering the French case and by giving a legal analysis of what goes into a national regulatory style. My main contribution, however, lies in the systematic exploration of the fate of these early regulatory styles in the wake of liberalization and Europeanization.

In addition to the policy case, I selected a number of country cases. This study seeks to trace the complex interaction between domestic and EU policymaking over time and, in doing so, it was unfeasible to include all twenty-seven member states. I chose to focus on France, Britain, Germany, and Italy because they are generally considered core states within Europe.[17] They are the largest European countries, as ranked either by their populations or their economies. Moreover, they are all longstanding members of the European Union. To the extent that liberalization and Europeanization have had an impact on regulatory styles, we would expect change to be observed in these cases and, vice versa, only if we observe change in these cases can a strong claim be made that a single *European* regulatory style is emerging.

This study relies on a variety of methods and sources to gather evidence on regulatory styles. I examined different types of legal texts: data privacy laws, implementing rules, internal agency regulations, agency decisions, and judicial decisions. To understand the rationale for the choice of different types of policy instruments, I drew on the official reports leading to the adoption of these laws, interviews with key policymakers, and the extensive secondary literature on data privacy in Europe. Understanding the day-to-day practice of policymaking and enforcement was more complex. Both qualitative and quantitative data were used: I conducted over thirty interviews with privacy officials and regulated parties and corresponded with them at different stages of the project. National privacy agencies all publish annual reports and these served as the source for data on enforcement actions and annual regulatory agendas. Last, I collected original data on privacy litigation by running searches in the major national electronic databases containing judicial decisions.

IV. Early Regulatory Styles

Data privacy emerged as a policy problem at virtually the same moment across Western Europe. The common trigger was the development of computer technologies that enabled governments to collect, store, and process vast quantities of data on their citizens. The fear was that the awe-inspiring capacity of these new databanks would be

[16] COLIN J. BENNETT, REGULATING PRIVACY (1992). Bennett shows that, in the United States, litigation rights were central to the regulatory scheme, while in Germany and Britain, regulators were styled as ombudsmen, with only soft powers of persuasion. In Sweden, a powerful privacy regulator was established, with a full complement of licensing and enforcement tools.

[17] Studies on the national dimension of EU policymaking typically include these four cases. *See, e.g.*, THATCHER, *supra* note 7; VIVIEN A. SCHMIDT, DEMOCRACY IN EUROPE (2006).

abused: wrong data could lead to unfair administrative determinations; personal data could be used by governments to control and manipulate their populations; rogue public officials could consult databanks for their own personal advantage. Economic actors were less of a threat than governments because of the limited availability of information technologies but some did have the resources to build large databanks—telecommunications companies, banks, and other large corporate actors—and they too were mistrusted. By the early 1970s, this commonly perceived threat gave way to a constant stream of government-sponsored expert committees and official reports. Reports were followed by legislation. And in the countries selected for this study, legislation was enacted in 1977 in Germany, in 1978 in France, and in 1984 in Britain. Italy was a laggard, due to general apathy to the policy problem and the instability of governing coalitions during the period, and it enacted data privacy legislation only in 1996, under pressure from the European Union. For this reason, I postpone all discussion of the Italian system until the later section on contemporary regulatory styles.

The core principles contained in these early privacy laws were remarkably similar.[18] Consensus emerged on four objectives: to guarantee oversight of databases, to ensure the accuracy of the personal data contained in computing systems, to protect data security, and to place limits on the collection, use, and storage of personal information. Through *oversight*, ordinary individuals would be empowered vis-à-vis the mammoth databanks containing their personal data. Transparency was key to oversight: the existence and the inner workings of all databanks had to be disclosed to the public. Access was also important to ensuring oversight: individuals were given the right to request their personal information and, if necessary, to correct or erase that information. The *accuracy* of personal data would protect against unfounded and manifestly unfair determinations based on that data. *Security* would prevent fraudulent uses of the personal data stored in computing systems. *Limitations* on collection, use, and storage would deter governments and large corporate actors from building databanks capable of violating basic liberties and controlling the population.

Notwithstanding these common principles, privacy was embedded in distinct legal frameworks. In Germany, data privacy fell squarely in the domain of constitutional law.[19] It was considered a fundamental constitutional right, part of the right to human dignity and the right to free development of personality. The impetus for data privacy legislation came largely from legal scholars who insisted that, as a matter of constitutional law, the government could not collect personal data without statutory privacy guarantees, and policymaking in the area was, and continues to be, conducted in the long, powerful shadow of the German Constitutional Court.

The contrast between Germany and Britain could not be starker. In 1984, when Britain enacted legislation, it did not have a tradition of fundamental rights, full stop, and

[18] BENNETT, *supra* note 16 at 95-115.

[19] This account is drawn from ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY 51-52, 63-69 (2008); Hans Peter Bull, *Datenschutz als Informationsrecht und Gefahrenabwehr*, NEUE JURISTISCHE WOCHENSCHRIFT, No. 23, June 6, 1979, pp. 1177-1182 , at 1181; Spiros Simitis, *Chancen un Gefahren der elektronischen Datenverarbeitung*, NEUE JURISTISCHE WOCHENSCHRIFT, No. 16, April 1971, pp. 673-682, at 675.

in the private sphere, it lacked a common law right of privacy.[20] The British law was adopted in response to external forces—to implement the Council of European Convention of 1981.[21] Although the conservative Thatcher government was wary of the regulatory burdens that would be created by the new scheme, it had very little choice but to sign and implement the Convention. The fear was that failure to join the Convention would give other countries reason to divert data flows away from Britain and therefore would undermine the competitiveness of British industry. In the regulatory practice that followed, data privacy was conceived largely as a matter of good corporate practices and responsible management of information systems, not as a question of individual rights. Indeed, in the 1980s, employees in the responsible administrative agency jokingly referred to privacy as the "p-word," a word that, as a matter of government policy, was never to be mentioned.[22]

In France, similar to Germany, privacy was considered a fundamental right (*liberté publique*). But the right to privacy, like most French rights, had a distinct republican flavor.[23] The origins of the French legislation are to be found in the popular outrage caused by the revelation of a number of mammoth government databases and the legislative drafting work of an elite government committee that was established in the wake of the scandal. In the French scheme, vindication of the right was not left to individuals and their lawyers but to public servants—the administrative agency created by the law and the criminal prosecutors tasked with pursing violations of the law. No French court had the power to entertain fundamental rights cases brought by individuals, not even the constitutional court. And individuals preferred to obtain redress as civil parties to criminal prosecutions rather than by independently bringing tort cases against those private firms and state officials that had violated their privacy rights.

The other important source of variation among early privacy systems, and the one that lies at the heart of this study, was the type of regulatory system established to implement data privacy safeguards. The subtleties of each country case are fully explored below, but let me preview the findings here. In all three cases, administrative agencies independent of the executive branch were created, driven by the logic of the policy area: the main party being regulated was the government and therefore enforcement could not be entrusted to an office within a government ministry, but rather had to be given to an independent, arms-length body. Nonetheless, the policy tools and administrative procedures employed by these independent agencies varied considerably and mapped onto the general patterns outlined earlier. The British case most closely approximated the flexible, cooperative model. The British privacy regulator served as an ombudsman, informally settling complaints brought by privacy victims, managed a

---

[20] This account is drawn from BENNETT, *supra* note 16 at 82-94; BRYAN NIBLETT, DATA PROTECTION ACT 1984 1-8 (1984); 1 ENCYCLOPEDIA OF DATA PROTECTION 1020/3-1024 (Rosemary Jay et al., latest update August 2009).

[21] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaties No. 108 (Jan. 1, 1981).

[22] Interview with Data Protection Registrar official, March 5, 2003.

[23] This account is drawn from GUY BRAIBANT, RAPPORT AU PREMIER MINISTRE, DONNÉES PERSONNELLES ET SOCIÉTÉ DE L'INFORMATION 31-32 (1998); DAVID FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 169-73 (1989).

registration system for databanks, and promoted industry self-regulation, so-called codes of practice. But it had no rulemaking power and few enforcement powers. The German system was similar to the British one: Self-regulation was absolutely central, privacy regulators served largely as ombudsmen, administrative enforcement powers were light, and rulemaking power was retained by the government. The French system was the most formal and hierarchical of the early privacy systems. There the privacy regulator had licensing, registration, and rulemaking powers and routinely used them to set down conditions for government and private-sector databanks. It had considerable investigation and sanctioning powers, although it rarely used them. And in contrast with Germany and Britain, self-regulation was absent and complaints mainly served as a trigger for agency enforcement, not as part of an informal dispute resolution system. Nowhere was litigation—brought to challenge administrative decisions or to enforce regulatory duties through tort suits—a significant component of the regulatory system.

a. France

At the epicenter of the French scheme was an independent, multi-member government commission (*Commission Nationale de l'Informatique et des Libertés* or CNIL) entrusted with extensive licensing, rulemaking, and enforcement powers.[24] The French law established a two-track system, one for private actors and another for public actors. Because the public sector was perceived as the main threat to privacy, its regulatory duties were the most onerous. Public databanks required a license (*avis favorable*) from CNIL, with a right of appeal to the Council of State (*un décret pris sur avis conforme du Conseil d'Etat*). In practice, CNIL rarely granted or denied licenses outright, but preferred to set down the conditions under which the proposed data processing would be lawful. To mention but one example, the decision authorizing the state telecommunications monopoly's billing system required that the last four digits of the numbers dialed be anonymized.[25] In the 1980s and 1990s, the majority of agency acts were decisions on these types of licensing applications—big public databases with information on housing, social security, political parties and more. The details of private databanks, by contrast, only had to be notified to CNIL, after which operations could commence. Both public and private databanks were entered into a public register open to individuals interested in discovering where their personal information was located and how it was being used. The public register was designed to foster transparency and to enable CNIL to keep abreast of trends in computer technologies and privacy threats.

Related to licensing and notification was the power to issue administrative regulations (*normes simplifiées*) specifying the privacy standards applicable to different types of databanks. These have been issued in areas such as personnel records, customer files, and survey data. An operator that follows the applicable regulation is spared the ordinary licensing and notification process and simply is required to file a declaration

[24] This overview of the regulatory framework is based on Act 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties; JEAN FRAYSSINET, INFORMATIQUE FICHIERS ET LIBERTÉS 76-77 (1992); ANDRÉ LUCAS, LE DROIT DE L'INFORMATIQUE 49 (1987).

[25] CNIL, Délibèration No. 82-104 du 6 juillet 1982 portant sur la mise en place d'un traitement automatisé de facturation téléphonique detailleé, Annual Report 1982 at 39, 242.

stating that it is in compliance. CNIL has made extensive use of this rulemaking power. According to one estimate, by 2002, approximately eighty percent of all data processing operations were covered by administrative regulations.[26]

Regulatory enforcement powers were substantial, although in practice they were used infrequently. These included the power to enter premises, inspect databanks and request documents, all without proof of wrongdoing and without the need to go to the courts for authorization.[27] Sanctions consisted in either a non-binding administrative warning (*avertissement*) or referral of the violation to the criminal prosecutor's office. An administrative complaints procedure existed but, in the French system, this procedure was conceived not as a form of informal dispute resolution, but as a means of detecting possible violations—a trigger for the enforcement system.[28] Despite these considerable powers, the record shows that they were rarely used. In the 1980s and 1990s, inspections averaged just 21 per year, warnings 2 to 3 per year, and referrals for prosecution under 1 per year. In short, the French privacy agency preferred to set down privacy guarantees for databanks through licensing and rulemaking rather than monitor and sanction for rule breaches, acting more as policymaker than policeman.

As for litigation, the background principles of administrative law and tort law applied. Even though, compared to other European systems, the French system is generous to plaintiffs, it does not have the punitive damages awards, class actions, and other litigation incentives of the American system, and therefore it should not come as a surprise that litigation rates were low.[29] There are no official sources on data privacy litigation and therefore I constructed a data set based on searches of the two major French electronic databases, starting in 1986 for administrative law challenges to CNIL decisions and in 1990 for statutory tort cases. In the 1980s and 1990s, challenges to CNIL decisions were sporadic: in many years, the number of cases decided was 0 or 1 and in no year was it higher than 5, for a total of 23 cases decided between 1986 and 1999. Statutory tort litigation was also minimal: a search for data privacy cases decided by the highest court (Court of Cassation) between 1990 and 1999 resulted in only 13 cases.

b. Germany

In contrast with France, when Germany adopted federal privacy legislation in 1977, it avoided a top-heavy licensing and registration system for databanks. Instead, consonant with German administrative tradition, policymakers opted for a system of self-regulation and negotiated compliance: internal compliance officers and industry association agreements, on the one hand, and informal dispute resolution by administrative agencies on the other hand.

---

[26] Interview with member of CNIL, October 19, 2002.

[27] These powers are analogous to American administrative inspections and American administrative subpoenas.

[28] *See, e.g.,* Annual Report 1986 at 35-37; Annual Report 1987 at 24-25.

[29] In French administrative law, the rules of standing favor plaintiffs because they do not need to show any particular harm in bringing challenges to administrative regulations. Under French tort law, breach of a statutory duty automatically constitutes a tort under the Civil Code, without the need to show other evidence of fault. Moreover damages for emotional distress (*dommage moral*) are routinely awarded.

Before proceeding with this discussion of the German regulatory style, a brief explanation of the complex bureaucratic organization of privacy regulation is in order. In line with German federalism, the original privacy law split public-sector oversight between a federal office with jurisdiction over the federal public sector and state (Land) agencies with jurisdiction over their Land public sectors.[30] Private-sector oversight, by contrast, was left entirely to the Länder. Although public-sector agencies were uniformly independent of the executive branch, given that the executive branch was the object of their oversight activities, private-sector agencies were generally part of the Land Ministry of Interior and subject to the ordinary hierarchical system of ministerial control and accountability. Only the small city-states of Bremen, Hamburg, and Lower-Saxony decided to consolidate public and private-sector oversight in a single, independent authority, more for reasons of administrative expedience than anything else. For purposes of brevity, the following discussion focuses on the legal powers of private-sector regulators and the analysis of how these powers have been used in practice relies mostly on information reported by the Hessian regulator.[31]

From the very beginning of the debate on what shape privacy regulation should take, self-regulation was emphasized as the key to good data privacy policy. The government's report on the proposed legislation was peppered with references to the principle of "self-responsibility and self-control" (*Prinzip der Selbstverantwortlichkeit und Selbskontrolle*).[32] Under the law, private firms were required to appoint an internal compliance officer who was responsible for keeping a record of the company's databanks, conducting employee training, and ensuring respect for the law.[33] This officer had to be an expert in computer technology and was guaranteed absolute independence from her employer. If the internal compliance officer needed advice on how to apply the legislation or faced resistance from her employer, she could turn for help to the privacy authority. These self-regulatory duties were strictly enforced: the reports published by the Hessian authority in the 1990s show that agency enforcement proceedings were routinely brought against companies that failed to appoint internal compliance officers and internal compliance officers that failed to comply with their statutory duties.

Another form of self-regulation was voluntary industry rules. This was not written into the data privacy law, but was and continues to be a common regulatory practice. In Germany, trade associations routinely submit model contracts and industry rules to regulators for their advice and informal approval and the data privacy field is no exception.[34] One prominent example in the privacy field is the so-called SCHUFA clause

---

[30] BUNDESDATENSCHUTZGESETZ [Federal Data Protection Law] [hereinafter BDSG] (1977) §§ 17, 29.
[31] Of Germany's sixteen Länder authorities, I chose to focus on the Hessian one because it has the best annual reporting system and is responsible for policing the financial services industry, typically a source of privacy concerns.
[32] BT-Drucksache 7/1027 at 18.
[33] BDSG 1977 §§ 28, 29.
[34] *See* Steven Casper, *The Legal Framework for Corporate Governance: The Influence of Contract Law on Company Strategies* in GERMANY AND THE UNITED STATES IN VARIETIES OF CAPITALISM 387, 396 (Peter A. Hall & David Soskice eds., 2001).

included in all contracts entered into between banks and their customers.[35] All German banks are participating members of a central clearing house on creditworthiness called SCHUFA (*Schutzgemeinschaft für Absatzfinanzierung und Kreditsicherung*), through which they pool and exchange data on their clients' credit history. This kind of data transfer must satisfy a number of legal conditions, including the duty to disclose transfers of personal information to banking customers and to obtain their consent. In the mid-1980s, a standard clause was developed to meet these legal requirements by the industry association for banks (*Zentraler Kredit Auschuss* or ZKA), in close cooperation with Hesse and other Land privacy regulators, and then was adopted as a matter of good business practice by all the member banks. Although this process does not result in an official administrative decision, both industry players and regulators consider the outcome of the process to be binding. The letter from the privacy agency approving the industry rules is treated as a definitive interpretation of the law, guiding agencies and the courts in their application of the law and giving firms that adhere to the outcome solid assurance of being in line with their legal duties.

The heavy reliance on self-regulation in German data privacy law might seem impossibly optimistic. Yet the German system is widely reputed to be among the best in Europe. To understand why, it is necessary to situate self-regulation in the data privacy arena in the larger institutional and economic environment in which it operates. In a coordinated market economy like Germany, economic life is highly organized and institutionally rich.[36] In contrast to liberal market economies like the United States and Britain, in which labor, technology, and capital are secured through arms-length, competitive market transactions, coordinated market economies like Germany and Sweden rely more heavily on coordination among firms and between labor and capital. Many public goods like education and vocational training that in a liberal market economy are provided by the state or not at all, are produced by economic actors.[37] One such public good might be said to be rulemaking and enforcement. Self-regulation entails a considerable degree of discretion and a firm that is part of a highly disciplined industry association in a coordinated market economy, risks opprobrium if it uses this discretion to tip the balance too far away from the regulatory goal, in the direction of firm profits.[38] Similarly, a firm that seeks to get around the discipline of an internal compliance officer by dismissing that officer faces all the hurdles of German labor law, an important feature of coordinated market economies.[39] In a liberal market economy like the United States, these organizational safeguards are generally not in place to incentivize firms to set stringent rules or to protect internal compliance officers from

---

[35] Interview with officials from the BVD (Association of Cooperative Banks), BDB (Association of Private Banks), and BOB (Association of Public Banks), July 3, 2003.

[36] Peter A. Hall & David Soskice, *Introduction*, in VARIETIES OF CAPITALISM: THE INSTITUTIONAL FOUNDATIONS OF COMPARATIVE ADVANTAGE 387, 396 (Peter A. Hall & David Soskice eds., 2001).

[37] *See* KATHLEEN THELEN, HOW INSTITUTIONS EVOLVE: THE POLITICAL ECONOMY OF SKILLS IN GERMANY, BRITAIN, THE UNITED STATES AND JAPAN (2004).

[38] *See generally* John D. Donahue & Richard J. Zeckhauser, *Public-Private Collaboration* in THE OXFORD HANDBOOK OF PUBLIC POLICY 496, 514-518 (Michael Moran et al. eds., 2006).

[39] For an overview of the German labor law system with a view to the termination decision, *see* Michael Kittner & Thomas C. Kohler, *Conditioning Expectation*, 21 COMP. LAB. LAW & POL'Y J. 263, 300-320 (2000).

employer pressure. In other words, in the German context, this type of self-regulation is a viable alternative to state enforcement, not necessarily the case in a liberal market economy like the United States.

Returning to German privacy authorities, they operated largely as ombudsmen, investigating and resolving privacy complaints, not as agenda-setters or policemen patrolling for regulatory breaches. The powers bestowed upon privacy authorities were limited. Their only direct form of rulemaking power was, and continues to be, non-binding, informal recommendations on good data privacy practices (known variously as *Orientierungshilf*e, *Richtlinie*, and *Empfehlungen*).[40] Enforcement was conceived entirely as an appendage to the informal settlement of privacy disputes by administrative authorities. Before a privacy agency could take any action, it had to receive an individual complaint.[41] These complaints would give rise to an investigation, which generally entailed a simple phone call or written notice, but also could escalate to a search of firm premises or an administrative subpoena for documents. If the dispute was not resolved informally, an administrative fine proceeding could be commenced for a limited subset of violations. Most regulatory breaches, however, were punished as criminal offenses and, unlike France where the privacy agency had the power to make criminal referrals, privacy victims themselves had to file a complaint with the prosecutor.[42] The practice of the Hessian authority underscores this consensual approach to regulatory enforcement: in the 1990s, individual complaints were routinely investigated, but most were settled amicably and few administrative proceedings were brought.[43] This emphasis on the routine resolution of privacy complaints through informal means distinguished the German privacy regulator from the French one and put it close to the British one, which as we shall see, operated a similar dispute resolution system.

In the original privacy scheme, litigation was left to the background law of regulatory offenses for challenges to administrative fines, and to the background law of statutory torts for individual suits against privacy violators. This changed in 1990, when the data privacy legislation was amended to facilitate tort litigation: the amendments made it somewhat easier to sue government agencies by allowing victims to recover without establishing fault, *i.e.*, negligence or intent, and they made it easier to recover against private tortfeasors by shifting the burden of proof on fault to the defendant.[44] Yet these changes had no impact on litigation rates, which remained low throughout the 1980s and the 1990s.[45] A search of the data privacy cases decided by the highest court with jurisdiction over civil and criminal matters (Bundesgerichthof) from 1977 to 2007 resulted in a trickle of one to three cases per year in the 1980s, followed by a dry spell in the 1990s, followed by another trickle of cases. The numbers on litigation before the highest labor court were even lower: between 1990 and 2007, a total of six privacy cases

[40] E-mail from Hans Tischler, Office of the Federal Data Protection Commissioner, April 15, 2009.
[41] BDSG 1977 § 29.
[42] *Id.* § 41.
[43] The Hessian annual reports were available starting in 1990.
[44] BDSG 1977 (as amended in 1990) §§ 7, 8.
[45] Although systematic data on administrative litigation were not available, it appears from the Hessian annual reports that firms occasionally challenged the administrative fines issued by the privacy regulator but that since there were relatively few fines, there was also little litigation.

were decided. Quite remarkably, none of the case reports in the data set, which also includes lower courts, mentions a damages award. In sum, as in France, private litigation was an insignificant component of the regulatory process.

c. Britain

The early British regulatory framework, enacted in 1984, rested on three components: registration, voluntary codes of practice, and administrative dispute resolution.[46] At the heart of British privacy regulation was a registration system managed by an independent government authority—the Data Protection Registrar. With only a few exceptions, the details of all public and private databanks had to be filed with the Data Protection Registrar and included in a public register, in the interest of improving transparency and enabling the privacy regulator to catch emerging privacy problems. The choice of an independent agency and a registration system was clearly influenced by the trend that had emerged in other European countries, all of which had independent privacy authorities and some kind of registration system.[47] At the same time, however, as in the German case, British policymakers rejected licensing and rulemaking, which existed in Sweden and France, but were perceived as bureaucratic and inconsistent with the informal and consensual British regulatory style.[48] And even the registration system alone proved a heavy burden for the Data Protection Registrar: throughout the 1980s, a huge proportion of the agency's resources were devoted to processing registration notices.

Enforcement powers, compared to France and Germany, were weak and were all tied to registration. If a registered party was found to be in breach of one of the data protection principles—the substantive duties imposed by the privacy law—the Registrar had the power to issue an injunction ("enforcement notice"), de-register the operator, effectively barring it from doing business, or prohibit the operator from transferring personal data abroad. Yet the latter two powers were never used, since they were considered too draconian, and enforcement notices were issued only infrequently—an average of three per year between 1987, when the power came into effect, and 1998, when the original law was overhauled. Moreover, the Registrar was handicapped by a lack of administrative investigation powers. Unlike French and German regulators, the British agency did not have the authority to inspect premises or compel information but rather had to apply for a court warrant based on evidence that there were "reasonable grounds" for suspecting a violation of the law. The Registrar could also bring criminal prosecutions seeking fines but this power did not extend to the majority of privacy violations and the level of the fines was extraordinarily low, originally a maximum of £2,000 and later £5,000.

---

[46] This overview of the British system is drawn from the Data Protection Act 1984 and NIBLETT, DATA PROTECTION ACT 1984, *supra* note 20.

[47] Sir Norman Lindop, *Report of the Committee on Data Protection*, Cmnd. 7341, HMSO, London, at 28-29, 171, 184 (Dec. 1978).

[48] *Id.* at 168 (licensing). Although agency rulemaking powers were originally proposed, the Thatcher government rejected them in favor of self-regulation and non-binding agency guidance.

The second major component of the British regulatory scheme was industry-sponsored codes of practice. In the original law, the Data Protection Registrar was instructed to encourage trade associations to develop their own codes of practice. In the years that followed, the Data Protection Registrar vigorously promoted industry codes of practice as an important tool for improving privacy standards[49] and industry associations routinely consulted the Registrar on their proposed codes, resulting in roughly sixteen by 1998.[50]

The last component of the regulatory scheme was informal administrative dispute resolution.[51] Under the original law, the Data Protection Registrar had a duty to look into any complaint involving a "matter of substance" and to attempt to resolve the matter. Since it was nearly impossible to determine from the face of a complaint whether a "matter of substance" had been raised, the Registrar's policy was to inquire into all complaints.[52] The dispute resolution system proved to be immensely popular: between 1984 and 1998, the number of complaints filed with the agency grew from 11 to 4,173 per year. This type of routine dispute settlement is familiar from the section on Germany but the British case is unusual in that the Registrar had virtually no discretion to ignore complaints and direct scarce agency resources elsewhere. In short, the British agency was styled as an ombudsman responsible for settling individual grievances, not as an agenda-setting policymaker or as a rule-enforcing policeman.

Even more so than in France and Germany, tort litigation was an insignificant part of British privacy regulation. This is principally because the background principles of English common law on statutory torts stand out as particularly stingy towards plaintiffs.[53] In common law systems, breach of a statutory duty does not automatically give rise to a right to sue in court as it generally does in civil law systems. Before a case may be brought, it must be demonstrated that the legislature, in enacting the statute, specifically intended to revamp the pre-existing common law framework by creating a new right of action. The easiest way for the legislature to do so is to write a statutory provision giving victims a right of action. And the drafters of the British privacy law limited this right of action to four, narrowly drawn classes of privacy breaches. Tort litigation rates reflected this carefully constrained right of action: according to a report from a specialized scholarly publication, there were only three cases seeking damages decided under the original British law.[54]

---

[49] *See, e.g.*, Data Protection Registrar, Annual Report 1985/86 at 9 (1986); Data Protection Registar, Annual Report 1987/88 at 18 (1988).
[50] *See* 4 ENCYCLOPEDIA OF DATA PROTECTION, *supra* note 20, §§5001-5361.
[51] *See, e.g.*, Data Protection Registrar, Annual Report 1986/87, at 26-27 (1987).
[52] Report by the Comptroller and Auditor General, Data Protection Controls and Safeguards, July 27, 1993, *reprinted in* 1 ENCYCLOPEDIA OF DATA PROTECTION *supra* note 20 at 4927-4964.
[53] Another reason that the British scheme was less plaintiff-friendly than the German and French ones was because compensation for pain and suffering ("distress") was only available if the plaintiff first proved that she had suffered tangible damages involving economic or physical harm.
[54] 1 ENCYCLOPEDIA OF DATA PROTECTION, *supra* note 20, at 1161.

V. Forces for Change

Since the 1970s and 1980s, when European data privacy regulation first took root, two dramatic changes have transformed the regulatory environment: the digital revolution, which is closely connected to market liberalization, and the Europeanization of policymaking. These forces have provoked change and convergence in all four national systems, moving them away from licensing and registration, and pushing them towards tough administrative enforcement of government standards and self-regulatory techniques. In this section, I explore how the new digital marketplace and the Europeanization of policymaking have fostered this pattern of regulatory convergence.

a. The Digital Revolution and the Transformation of the Marketplace

The rise of digital technologies and the exponential growth of computing power have dramatically altered the nature of the data privacy regulatory problem. Early on, only governments and large corporate actors like banks and telecommunications operators had the technological capacity necessary to process large quantities of data. Now, however, that the technology has become so sophisticated and cheap, everyone can collect, duplicate, store, and communicate vast quantities of digital information, anywhere in the world. This has led to a host of new challenges for privacy regulators, the most important one for our purposes being the proliferation of market actors caught by privacy rules. Today, not just the telephone company knows your personal habits, but the bookstore, the travel agent, and every other service and goods provider that operates over the internet. Although in some respects these challenges are exceptional, the difference between privacy and other regulatory areas should be understood as one of degree, not in kind. Market liberalization in Europe was driven by the extraordinary possibilities that digital technologies created for telecommunications, financial services, and other economic sectors, and, as a result, these new markets parallel the broader digital universe: densely populated and complex, with a rapidly changing set of services and products on offer.[55] The market constraints that have shaped contemporary regulatory styles in the privacy arena are broadly similar to those in other policy areas and therefore the privacy case should be understood as belonging to the more general phenomenon of market liberalization.

The proliferation of regulated parties in the data privacy arena is directly responsible for one major shift in European regulatory styles: national systems like France that previously relied on registration and licensing have had to drastically curtail the scope of application of these regulatory tools. Too many individuals and firms are caught by blanket registration and licensing requirements for administrative agencies to be able to review registration notices and licensing applications in a meaningful way. Registration and licensing were originally adopted because they were believed to be flexible tools that would allow regulators to keep abreast of the changing digital environment and to respond, on a case-by-case basis, to new information systems. However, they are also resource-intensive policy tools that can only work in a cozy

[55] VOGEL, FREER MARKETS, MORE RULES, supra note 7 at 25-42.

regulatory environment of few actors and many government watchdogs, one which no longer exists in the privacy field.

In a parallel process, the new digital environment has rendered other regulatory instruments more attractive. The sheer number of corporate actors that today come under the umbrella of data privacy regulation has fostered a style of regulatory enforcement oriented more towards deterrence than towards the management and remediation of breaches. As we shall see, administrative inspections and regulatory sanctions are on the rise across all four national systems and one of the justifications for this shift has been the impossibility of inducing the numerous corporations caught by the rules to take privacy regulation seriously without the threat of enforcement actions. The managerial, problem-solving approach to enforcement of the past, with informal requests for information on corporate practices, individualized recommendations on how to improve privacy, and prospective administrative orders, setting out the steps necessary to come into compliance, is no longer perceived as adequate.

The same market trends have also prompted national officials to promote self-regulatory techniques. To some extent, the impulse is to alleviate the burdens placed on over-taxed, under-resourced, government officials by shifting regulatory responsibility to the business community itself More importantly, however, is the appreciation that in a context of extreme diversity, corporations are better placed than government to design and monitor the specific standards that are appropriate to their particular brand of digital technologies and privacy threats. As will be discussed in greater detail below, a variety of self-regulatory techniques have emerged: internal corporate compliance officers, self-regulatory codes adopted by industry associations, privacy seal programs that seek to use markets to reward good corporate practices, and privacy management systems comparable to the ones that have been introduced in environmental protection. These techniques differ in important respects, some representing traditional patterns of government-industry relations and others informed by contemporary thinking on responsive regulation, but they all allow for more industry initiative than classic command-and-control regulation.

b. The Europeanization of Policymaking

Although the new market environment is conducive to tough enforcement and self-regulation, the widespread adoption of these strategies has also been driven by the politics of Europeanization. Notwithstanding their intrinsic appeal, policymakers still have a variety of regulatory options available to them and domestic regulatory styles are not easily malleable, embedded as they are in a thick set of institutions and cultural practices. Indeed, in many places, the punitive tactics of tough enforcement and the private empowerment entailed by self-regulation have traditionally been suspect. Thus, to understand why these regulatory strategies have been accepted across a broad range of national systems, it is necessary to turn to the legislative and regulatory politics of Europeanization.

In 1995, the European Union became involved in the policy area for the first time, with the adoption of the EU Privacy Directive.[56] This has since been complemented by a series of sector-specific measures in telecommunications, police cooperation, and other areas, but the Directive continues to serve as the basic framework that guides all other policymaking in the field. Although day-to-day implementation and enforcement was left to national authorities, the Directive's drafters sought to guarantee that the privacy right would be adequately protected by setting down a common set of enforcement powers and redress mechanisms that had to be available nationally. Their choices were influenced both by policy diffusion mechanisms and by the need to create credible commitments to safeguard against national defection at the implementation phase. To the extent that these choices were compatible with the demands of the new digital marketplace, they have since shaped national regulatory styles. The Privacy Directive also set into motion a governance process responsible for overseeing national implementation and this process has fostered convergence in ways similar to the earlier experience with drafting the Directive.

1. The Privacy Directive

i. Policy diffusion

As has been demonstrated elsewhere, EU policies are rarely decided from scratch, but rather are shaped by competition among member states to incorporate their existing regulatory models into EU legislation.[57] Two important elements of the Privacy Directive were the product of transfer of national regulatory models to the whole of the European Union: the decision to include licensing and registration and the requirement that industry associations be allowed to come forward with self-regulatory codes of conduct.

The provision on registration and licensing was one of the most controversial in the Directive. [58] The original proposal, heavily influenced by the flexible German system, included no licensing and extremely limited registration requirements.[59] But when France, seeking to protect its existing regulatory system, opposed the proposal, it was modified to include extensive registration and licensing requirements.[60] Even though Britain, Germany, Ireland, Denmark, and a number of other northern countries doggedly fought this provision, on the grounds that it was unworkable and bureaucratic, it ultimately survived because of a narrowly tailored compromise designed to accommodate Germany, the most powerful member of the opposition. [61]

---

[56] Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data [hereinafter "Privacy Directive"], 1995 O.J. (L 281) 31.
[57] *See* Tanya Börzel, *Pace-Setting, Foot-Dragging, and Fence Sitting*, 40 J. COMMON MKT. STUD. 193 (2002).
[58] Privacy Directive, arts. 18-21.
[59] Proposal for a Council Directive , arts. 7, 11, 1990 O.J. (C 277) 3 [hereinafter 1990 proposal].
[60] Resultats des travaux of Groupe des "Questions économiques" (Protection des données), Council Doc. 10503/91, Jan. 20, 1992; Amended Proposal for a Council Directive, arts. 18, 19, 1992 O.J. (C 311) 30.
[61] *See, e.g.*, Transmission note from the Danish, German, Irish, and United Kingdom delegations to Working Party on Economic Questions (data protection), Council Doc. 9345/93, Oct. 15 1993, at 5.

In this saga, the coercion and emulation mechanisms that have been identified in theories of international policy diffusion were at work.[62] France and Germany had no intention of making the costly changes necessary to rework their regulatory systems and, as the most powerful countries in the European Union, they could use their clout to ensure that their national systems would be included in the Directive. Yet the voting rules in the Council of Ministers are such that France could not have imposed licensing and registration without support from a qualified majority of member states. And this qualified majority came from countries with common administrative law traditions—Greece, Italy, Spain, Belgium, and Luxembourg—most of which did not yet even have privacy legislation but nonetheless emulated the French position based on institutional and cultural affinities. Ultimately, however, the powerful diffusion process that occurred in the legislative negotiations has not had a significant impact on national regulatory styles, and this is because registration and licensing have been undercut by the other major force for change, the digital revolution. Policymakers in Britain, France, and Italy have all found registration and licensing to be unworkable and therefore they have devised myriad ways of whittling down these requirements, leaving little of the Directive's original scheme in place.

The other product of policy diffusion, industry self-regulatory codes, has been more successful.[63] Although these were already common regulatory practice in the Netherlands, Germany, Britain, and other northern countries, they are new to France and Italy, known to have closed administrative systems. In the Council of Ministers, the Dutch delegation pushed for the adoption of their system of government-approved industry codes, portraying them as a highly effective regulatory technique.[64] Its proposal received universal support from the other national delegations, in part because codes of conduct were seen as a convenient device for extending the reach of privacy principles, and in part because the cost of adapting national regulatory systems was minimal.[65] In the case of self-regulatory codes of conduct, the policy diffusion mechanism was not coercion or emulation, but policy learning: the drafters sought to draw on the lessons of the successful experience of one country in designing a common EU regulatory framework.

ii. Credible commitments

Another important set of choices concerned the structure and powers of national privacy agencies: they were required to act independently and to be endowed with a broad set of enforcement powers.[66] This Directive provision has had far-reaching consequences, for, in all four country cases, governments have been compelled to expand the administrative enforcement powers available to their regulators, and, in Germany,

---

[62] *See* Simmons, Dobbin & Garrett, *supra* note 13.
[63] Privacy Directive, art. 27.
[64] *See* Resultats des travaux of Groupe des "Questions économiques" (Protection des données), Council Doc. 7601/02, July 13, 1992.
[65] Interview with member of British delegation, March 3, 2003; interview with member of Italian delegation, April 13 & 14, 2003.
[66] Privacy Directive, art. 28.

privacy agencies have acquired greater independence from the executive branch. The negotiating history of these requirements strongly supports the credible commitments theory of institutional design in the European Union. In this literature, the European Commission and, to a lesser extent, the European Parliament are portrayed as the institutions responsible for the monitoring and sanctioning vital to credible commitments because of their impartial, supranational composition.[67] Therefore, it is significant that, consistent with the theory, independence and enforcement were incorporated at the behest of the European Commission and the European Parliament, not the member states, and that these requirements were justified as necessary for protecting the privacy right at the national level.

As explained above, independence was a common feature of European privacy regulation with the exception of Germany, where private-sector oversight at the Land level was generally located in the Ministry of Interior. German privacy advocates were highly critical of this system and, together with the European Commission, they pushed for language stipulating that privacy agencies had to be independent.[68] This was justified as critical to making EU law and privacy rights effective on the ground. In the Directive negotiations, Germany vigorously defended its system, with the other delegations passively looking on at what was perceived as a purely local dispute over how to structure the German regulatory system.[69] In fact, in the final version, the independence clause was considerably softened so that it only stipulated that regulators "act independently" but not that they be given structural independence through appointment and removal safeguards and other institutional devices.[70] Yet even so, as we shall see, Germany has continued to face pressure from German privacy advocates and the European Commission to grant complete independence to Land regulators, so powerful is the association between institutional independence and member-state compliance in European governance.

Like independence, the catalogue of enforcement powers was supported by the Commission, this time in conjunction with the European Parliament. Inspired by the consensual and managerial German model, the agency powers contemplated in the original Directive proposal were minimal, focusing mainly on the power to investigate possible privacy breaches and obtain information from data processors.[71] However, the European Parliament objected that this would make for weak enforcement of the right to privacy and it advocated a more comprehensive catalogue of powers.[72] With the backing of the European Commission, this catalogue of powers is what survived in the final version of the Directive.

---

[67] *See, e.g.*, Jonas Tallberg, *Paths to Compliance: Enforcement, Management, and the European Union*, 56 INT'L ORG. 609 (2002).

[68] Interview with German privacy expert consulted by European Commission, July 1, 2003; interview with European Commission official, October 30, 2002.

[69] Note from the German delegation to the Council, Council Doc., 6733/93, May 19, 1993; interview with member of British delegation, March 3, 2003.

[70] Note from the President to Permanent Representatives Committee, Council Doc. 6856/94, May 18, 1994.

[71] 1990 proposal, art. 26.2.

[72] Interview with European Commission official, October 30, 2002.

iii. Litigation

One area in which the Directive did not have much of an impact was litigation. The litigation provision closely tracked the German system for statutory privacy torts: individuals were given a right of action in the courts for all violations of their national privacy legislation and the burden of proof on fault, *i.e.* intent or negligence, was shifted from the plaintiff to the defendant.[73] As we shall see, this provision prompted litigation-friendly innovations in Britain. But on the whole, it is remarkable for what it did *not* do: fault remained an element of the tort, even though delegations like the French one supported an objective, no-fault standard that reflected their existing system of statutory liability.[74] Although the Commission proposed that courts be required to award damages for emotional distress, the final version of the Directive left the matter entirely to the discretion of the member states.[75] And innovations such as minimum damages awards and fee-shifting provisions, styled after the American system, were never even mentioned as a possibility. These attempts to improve litigation opportunities for privacy victims went nowhere because of the constant opposition of the member states: national delegations were uniformly reluctant to change their existing systems of tort remedies, partially because of the fear of increased litigation, and partially because of the desire to avoid the unanticipated consequences that any disruption of their traditional systems of private law and civil litigation could provoke.[76] This unsuccessful experience with negotiating a more plaintiff-friendly tort system is illustrative of the larger difficulties that have been encountered by the European Commission in attempting to harmonize tort remedies in consumer law, environmental protection, and others areas of the law. There is considerable resistance to tinkering with what is perceived to lie at the core of national legal systems.

2. EU Governance

In the European Union, new policies typically bring with them a host of governance mechanisms designed to oversee compliance and to enable regulatory adaptation to changing circumstances. In data privacy, the governance process comes in two distinct institutional forms: centralized oversight by the European Commission and a decentralized network of national privacy regulators, called the Article 29 Working Party.

Agency independence and deterrence-oriented enforcement have been pushed by both the Commission and the Article 29 Working Party. In 2002, the Commission conducted a comprehensive review of the Privacy Directive. The outcome was a ten-point work program for improving national implementation in which one of the centerpieces was administrative enforcement—and not litigation, alternative dispute

[73] Privacy Directive, art. 23.
[74] Resultats des travaux of Groupe des "Questions économiques" (Protection des données), Council Doc. 5594/93, April 1, 1993.
[75] Interview with European Commission official, October 30, 2002.
[76] Interview with member of British delegation, March 3, 2003.

resolution, licensing, and any number of other possible regulatory tools.[77] Shortly thereafter, the Commission prosecuted Britain and Germany for breaches of the Privacy Directive, Britain for not having endowed its privacy regulator with adequate investigative and sanctioning powers and Germany for not requiring that Land regulators be independent. And when, in 2007, the Commission revisited national implementation of the Privacy Directive, its attention was again squarely on enforcement and independence:

> One concern is respect for the requirement that data protection supervisory authorities act in complete independence and are endowed with sufficient powers and resources to exercise their task. These authorities are key building blocks in the system of protection conceived by the Directive and any failure to ensure their independence and powers has a wide-ranging negative impact on the enforcement of the data protection legislation. [78]

Tough enforcement by agencies independent of political direction is clearly understood by the Commission to be the *sine qua non* of effective data privacy regulation.

The Working Party has also pushed national authorities to take a more aggressive approach to privacy violations. Among its many enforcement initiatives, it organized a closed, hands-on workshop of privacy regulators in which the Spanish authority, known as the toughest of all European regulators, explained how it conducts inspections and assesses fines.[79] Moreover, the Working Party has begun to stage joint investigations involving national privacy agencies across the European Union. In 2007, after concluding its first joint privacy investigation, the Working Party strongly urged national regulators to use their inspection powers more aggressively and to go directly to firm premises to obtain access to corporate records and databases. [80]

The insistence of both the Commission and the Working Party on tough regulatory enforcement—something which, as we have seen, was entirely alien to early national regulatory styles—can only be understood in light of the credible commitments logic analyzed earlier. Implementation of privacy policy lies entirely in the hands of national governments and aggressive regulatory enforcement is one means of circumventing their policy discretion and ensuring that privacy rights are being enforced equally everywhere. International policymakers, unlike national legislators, cannot rely on the allocation of financial resources and a common party affiliation to guarantee that policymaking will be followed by executive-branch implementation. Rather, independence, administrative inspections, and sanctions have come to serve as alternative commitment devices.

---

[77] European Commission, First report on the implementation of the Data Protection Directive (95/46/EC), COM (2003) 265 final, May 15, 2003.
[78] European Commission, Communication on the follow-up on the Work Programme for better implementation of the Data Protection Directive, COM(2007) 87 final, March 3, 2007 at 5.
[79] Interview with European Data Protection Supervisor, January 25, 2010.
[80] Article 29 Data Protection Working Party, Report 1/2007 on the First Joint Enforcement Action, June 20, 2007.

Self-regulation has also been promoted, generally beginning with initiatives taken by northern countries with a tradition of self-regulation, and then spreading through the network of privacy regulators to other member states. For instance, the British regulator has championed two, related initiatives to encourage firms and government agencies to routinely build privacy guarantees into their information systems through critical self-evaluation, stakeholder consultation, and creative privacy engineering —Privacy Impact Assessments and Privacy by Design.[81] These policy ideas have been put forward by the British regulator in a variety of European forums, including the annual meetings of European data protection commissioners, and are becoming increasingly popular among other national regulators too.[82] Privacy seal programs are another example of the diffusion of self-regulation through European networks. A privacy seal is an official mark of good corporate practice that goes beyond the statutory minimum. To obtain a privacy seal, firms must generally compile information on their privacy safeguards, draft a privacy statement designed for their customers, and be inspected by an independent auditor. Privacy seals have been championed by the Privacy Commissioner of Schleswig-Holstein, which first established a privacy seal program locally and then obtained EU funding to develop a European privacy seal, as the leader of a Europe-wide consortium.[83] The French privacy agency has joined this consortium and has encouraged French business to take part in the program, and thus we see that this German initiative has begun to gain traction in other member states too.

VI. Contemporary Regulatory Styles

Even though Europeanization and the digital revolution have given rise to convergence, these common forces have been experienced differently in each country case. This section traces the national pathways through which policymakers have cut back on licensing and registration, moved from negotiated to deterrence-oriented regulatory compliance, and, in France and Italy, come to promote self-regulation as a complement to state-imposed rules. In each country, reform has proceeded through both major legislative innovation and the routine policymaking efforts of privacy regulators.

a. France

When the new French privacy law was passed in 2004, it was universally understood as moving the French system away from so-called *ex ante* regulation—preventing privacy violations through licensing—and towards *ex post* regulation—reacting to privacy breaches by conducting investigations and punishing offenders.[84] The new law eliminated the original two-track scheme of licensing for the public sector and notification for the private sector and replaced it with a narrow licensing requirement (*autorisation*), applicable only to those types of operations thought to present special privacy risks, and a general registration duty (*notification*), applicable to all other

[81] Information Commissioner's Office, Privacy Impact Assessment Handbook, December 11, 2007; Information Commissioner's Office, Privacy by Design, November 2008.
[82] European Privacy and Data Protection Commissioner's Conference, Edinburgh, April 23-24, 2009.
[83] Information on the European Privacy Seal *available at* www.european-privacy-seal.eu.
[84] Act 2004-801 of 6 August 2004.

operations. And since the agency's rulemaking power was retained, very few operations today are caught by either licensing or registration. At the same time, the array of administrative sanctions was dramatically expanded: administrative injunctions, administrative fines, orders blocking data processing, and temporary injunctive orders were all added to the French regulatory toolbox.

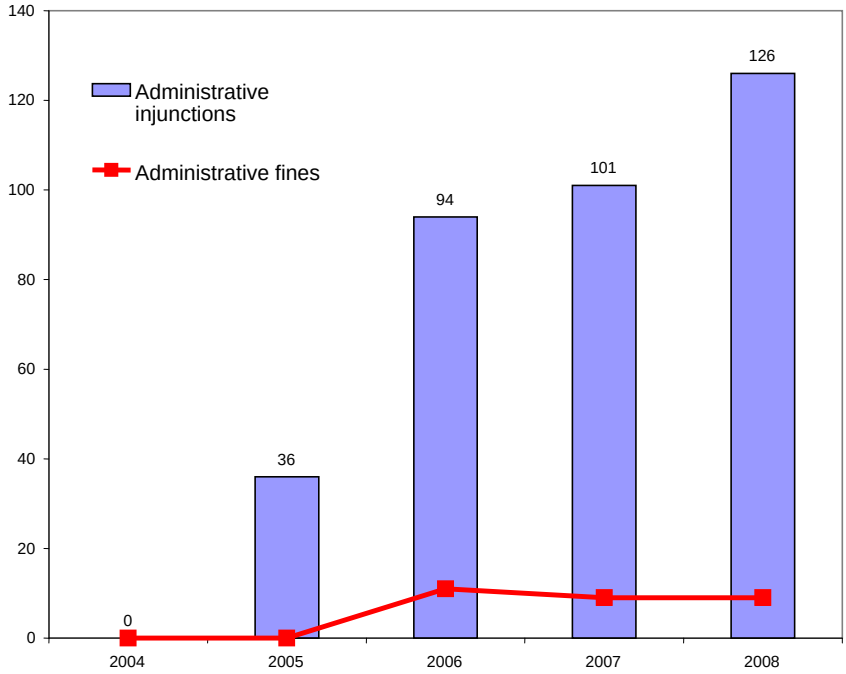
This new *ex post* regulatory philosophy has been enthusiastically embraced by the French privacy agency (CNIL). Its previously meek approach to enforcement has been replaced by a tough strategy of widespread government inspections and administrative sanctions for rule-breakers. The diagram below contains data on the number of administrative inspections carried out annually by CNIL. Throughout the 1990s, the numbers were low, but after 2004, when the new privacy law was passed, they sky-rocketed.

Source: CNIL, Annual Reports

The next chart shows annual figures for administrative injunctions and administrative fines, both of which were new powers introduced in 2004. The numbers on administrative injunctions are high and show a constant upwards trajectory, while the numbers on administrative fines are significant but lower since fines can be assessed only

after an operator fails to come into compliance with an injunction.

CNIL — Administrative injunctions and fines 2004-2008



Source: CNIL, Annual Reports

What has driven French policymakers to re-engineer their data privacy system? Compliance with the EU Directive was one motivating factor, since the specifics of registration, licensing, and enforcement were somewhat different from the French law.[85] The principal rationale, however, was the mismatch between a system centered largely on the licensing of big public databanks and the new digital marketplace. The view among French policymakers was that the old regulatory scheme had to be retooled to reflect the new reality of widespread data use throughout the public *and* private sectors and that what was needed was not more licensing, which was considered impracticable, but tougher sanctions to deter corporations from flouting the rules.[86] Thus they introduced a wide range of sanctioning powers that have been vigorously applied by a regulatory agency that likewise views deterrence as necessary for inducing corporate actors to take their privacy duties seriously.

In addition to the shift from *ex ante* to *ex post* regulation, the French system now carves out significant space for self-regulation. In the new law, French policymakers looked to the example of Germany to design a system in which corporations that appoint internal compliance officers are exempted from licensing and registration. CNIL has

[85] BRAIBANT, *supra* note 23 at 52; interview with CNIL official, October 15, 2002; interview with CNIL official, October 23, 2002; interview with Ministry of Justice official, October 21, 2002.
[86] *Id.*

taken extraordinary steps to encourage this self-regulatory practice by creating a special agency department to assist internal compliance officers and conducting regular training programs, with the result that, by the end of 2008, there were almost one thousand internal compliance officers.[87] Again taking the lead from Germany, the new French law established an official privacy seal program and, as mentioned earlier, the French regulator has partnered with the Schleswig-Holstein Privacy Commissioner to develop and administer a Europe-wide privacy seal. Furthermore, self-regulatory industry codes were introduced to comply with the Dutch-inspired provision of the Directive. So far CNIL has approved two industry codes, both related to direct marketing, and it is considering two others on call centers and commercial solicitations.[88] Mention should also be made of CNIL's efforts to encourage AFNOR, the French industry association responsible for technical standards, to develop privacy standards. Taken together, this flurry of activity represents a dramatic transformation of the relationship between French regulators and market actors and it is clear from the legislative debates that international policy diffusion has contributed to the trend.[89] The fact that these instruments had already been adopted elsewhere in Europe and appeared to have worked well there was a powerful rationale for experimenting with those same instruments in France.

To conclude this discussion of the contemporary French regulatory style, let us dwell for a moment on what did not change—litigation. The government report that prepared the way for the new privacy law proposed that it include a provision making statutory violations into strict liability torts, reasoning that such a change would better further the purposes of the Directive.[90] Yet this proposal never went anywhere and therefore, as before, privacy violations are litigated under the standard background rules on statutory torts. This aborted reform attempt is reminiscent of the debates on the original French law in the 1970s. The government report that preceded the original law proposed facilitating tort litigation based, tellingly, on the American system of generous standing rules and one-way fee-shifting arrangements (meaning that defendants bear their legal costs and attorneys fees, regardless of the outcome of the litigation).[91] But this pro-plaintiff recommendation was summarily dismissed. In other words, French lawmakers are extraordinarily constant in their resistance to anything that deviates from the standard tort regime that has been developed under the Civil Code.

Unsurprisingly, litigation rates in the 2000s showed no increase over the 1980s and 1990s. Between 2000 and 2007, the number of statutory tort cases decided annually by the Court of Cassation has ranged between 2 and 3. During the same time, the number of administrative law challenges to CNIL decisions has ranged between 0 and 3.

b. Germany

[87] CNIL, Annual Report 2008 at 43.
[88] CNIL, Annual Report 2005, at 32; CNIL, Annual Report 2007 at 41.
[89] *See* Senate Report No. 218 at 43 (2002-2003); National Assembly Report No. 1537 at 8, 25-28 (2004).
[90] *See* BRAIBANT, *supra* note 23 at 122.
[91] RAPPORT DE LA COMMISSION INFORMATIQUES ET LIBERTÉS (décret no. 74.938 du 8 novembre 1974) (1975), Annex at 32.

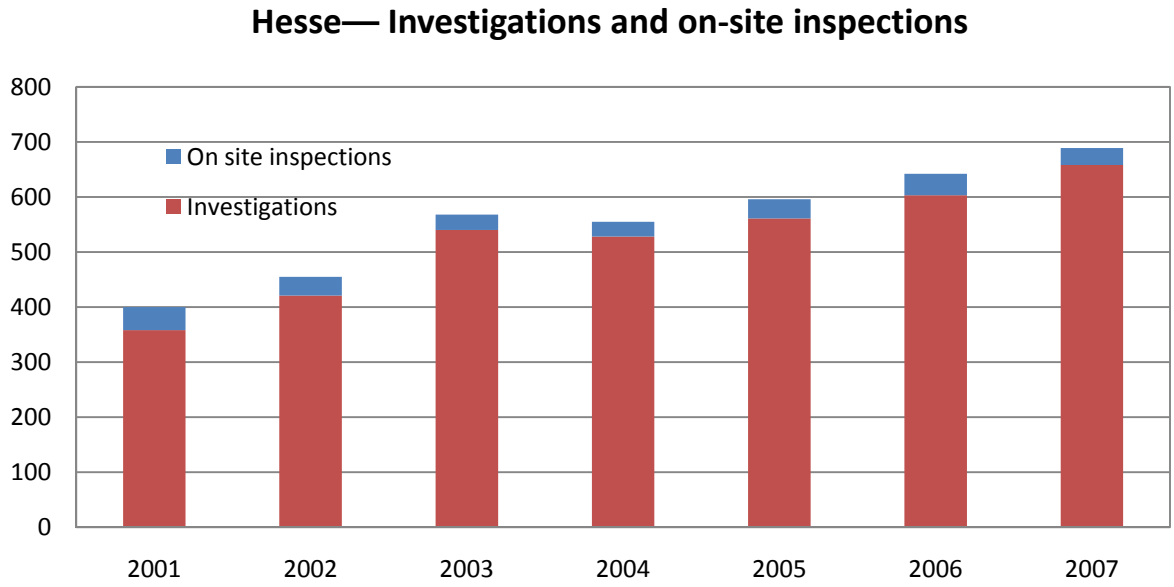
As elsewhere, in Germany, the self-regulatory and administrative enforcement components of data privacy regulation have been enhanced over the past decade. However, the most remarkable aspect of the German experience compared to the other country cases is the stability of its regulatory model. As before, data privacy policy is implemented through a combination of self-regulation, informal dispute resolution, and steady administrative enforcement, all set in the broader context of a hard, constitutional right to data privacy.

The new federal privacy law, enacted in 2001, significantly expanded the enforcement powers of private-sector regulators at the Land level.[92] In the new scheme, administrative enforcement is no longer inextricably linked to informal dispute resolution, but rather can be independently and strategically deployed by privacy regulators. While before administrative investigations had to be triggered by an individual complaint, regulators can now investigate suspected privacy infringements on their own initiative and, if administrative sanctions alone are considered inadequate, they have the power to refer violations to the criminal prosecutor's office. The fining powers of private-sector regulators have also been expanded considerably. Before most violations of privacy law were treated as criminal offenses, but in the new law, the vast majority have been converted into administrative offenses, with the few remaining criminal sanctions being reserved for offenses committed with an especially culpable state of mind.

These improved powers were all added to comply with the EU Directive.[93] The exclusively external origin of change sets Germany apart from the rest of the country cases, where tougher administrative enforcement has been driven not only by EU politics but also by domestic dissatisfaction with old regulatory tools. In contrast, German policymakers were fairly content with existing compliance levels and moved to improve investigation and sanctioning powers only when pushed to do so by Europeanization.

It appears that German regulators are making moderate but consistent use of their enforcement powers. The first graph shows the number of investigations and on-site inspections that were conducted annually in Hesse. Notwithstanding the recent decoupling of enforcement from dispute resolution, most investigations are still begun in response to individual complaints and therefore, in contrast with the other country cases, what is reported as an investigation can be as simple as a quick telephone call to the alleged offender. However, on-site inspections were also reported, and since an on-site inspection represents a fairly aggressive regulatory strategy, these figures give an idea of the administrative resources that were devoted to formal and adversarial regulatory enforcement as opposed to negotiated compliance. It is obvious that compliance is coming to absorb a growing amount of administrative resources and that adversarial tactics are part of the repertoire of agency action. At the same time, the low ratio of inspections to investigations overall suggests that the Hessian regulator continues to prefer informal avenues of dispute resolution and that the traditional German regulatory style of negotiated compliance is eroding only slowly.

[92] Bundesdatenschutzgesetz, May 22, 2001, BGB1. I.
[93] Interview with Federal Ministry of Interior official, July 8, 2003.



Source: Hesse, Annual Reports

To get an idea of what is happening outside of Hesse, there is one study available on sanctions throughout Germany in 2002-2007. The results are reproduced in the table below. These figures show that administrative sanctions are not simply a matter of law-on-the-books but rather are consistently applied by the Land authorities and can be expected to have a deterrence effect. However, the numbers are low given the size of the German population and again they suggest that the managerial German enforcement style is slow to change.

Germany—Regulatory sanctions, 2002-2007

Year	Regulatory sanctions
October 2002-August 2003	34
September 2003-August 2004	77
September 2004-August 2005	51
September 2005-August 2006	49
September 2006-August 2007	45

Source: Evelyn Seiffert, Hamburg Authority, "Bussgelder und Strafanzeigen"

Agency independence, the other component of a legalistic regulatory style, has also improved over the past decade. As was explained earlier, the German government successfully resisted structural independence for privacy authorities in the EU Directive and therefore, going by the formal letter of the law, nothing had to change in Germany to come into compliance. However, in the 1990s and 2000s, a number of German legal scholars and data protection officials used the Directive's independence provision to

argue that private-sector oversight had to be transferred from Land ministries to Land data protection commissioners (which are independent but only have jurisdiction over the public sector). [94] Although they did not prevail in the debates on the new federal law, they successfully persuaded a number of Land governments to transfer all regulatory power to their independent data protection commissioners.[95] Moreover, as was discussed earlier, the European Commission has prosecuted Germany for breaching the Directive and therefore, depending on the outcome of the case, all Länder might yet be forced to switch to a system of independent privacy agencies.[96] Here we see how the logic of credible commitments and the understanding of administrative independence as key to the rigorous enforcement of EU law have played out on the ground in Germany.

The drafting of the federal privacy law was also taken as an opportunity to experiment with new self-regulatory devices, in line with Germany's cooperative regulatory style. In addition to the existing devices of internal compliance officers and industry agreements, the new legislation mandated a privacy seal program. More importantly, an official report was commissioned from a group of German legal scholars on strategies for modernizing German data privacy regulation, designed to inform a second wave of privacy reforms once the immediate necessity of implementing the Directive had passed.[97] The report consisted entirely of recommendations for new forms of self-regulation and although the government has yet to implement these recommendations, they have been roundly applauded by the German community of privacy experts and data protection commissioners.[98]

The last point to make is that, as in France, nothing has altered on the litigation front. There were no significant changes made to litigation rights in the new law and the level of tort litigation for statutory privacy violations remains low. To give an idea of the litigation component of German privacy regulation, the table below shows the annual number of statutory tort cases in my data set that were brought in the main court system, which has jurisdiction over both civil and criminal litigation but not labor cases. For feasibility reasons, the data on the highest court (Bundesgerichthof) go back to the time of the enactment of the original federal privacy law while the data on the lower courts start in 1990. (The courts of first instance are the Amtsgericht for low-value claims and the Landgericht for high-value claims and the courts of appeal are the Landgericht and the Oberlandesgericht.) As the table demonstrates, litigation remains minimal.

---

[94] *See, e.g.*, Spiros Simitis, *Privatisierung und Datenschutz*, DATENSCHUTZ UND DATENSICHERHEIT 1995, 648-652; Ulf Bruhann & T. Zerdick, *Umsetzung der EG-Datenschutzrichtlinie*, COMPUTER UND RECHT 1996, S. 429-436.

[95] Mecklenburg-West Pomerania, Saxony, Rhineland-Palatinate, Northrhine-Westphalia, Schleswig-Holstein, and Berlin have recently adopted this model. In all, nine Länder (those already mentioned plus Hamburg, Bremen, and Lower Saxony) operate with a single authority and seven operate with regulatory jurisdiction split between two authorities (Baden-Württemberg, Brandenburg, Saarland, Bavaria, Thuringia, Hessen, and Saxony-Anhalt). *See* E-mail from Hans Tischler, Office of Federal Data Protection Commissioner, April 15, 2009.

[96] Case C-518/07, Commission v. Germany, 2008 O.J. (C 37) 8.

[97] Alexander Rossnagel, Andreas Pfitzmann, Hansjürgen Garstka, Modernization of Privacy Law, Legal Opinion Commissioned by the Minister of Interior, Berlin 2001.

[98] *See* E-mail from Hans Tischler, Office of the Federal Data Protection Commissioner, April 15, 2009.

Germany—Cases decided, 1978-2007

Year	First Instance	Second Instance	Supreme Court	Year	First Instance	Second Instance	Supreme Court
1978	Nd	Nd	1	**1993**	0	1	0
1979	Nd	Nd	0	**1994**	1	1	0
1980	Nd	Nd	0	**1995**	1	1	0
1981	Nd	Nd	2	**1996**	3	3	0
1982	Nd	Nd	2	**1997**	2	3	0
1983	Nd	Nd	3	**1998**	4	2	0
1984	Nd	Nd	1	**1999**	1	1	0
1985	Nd	Nd	2	**2000**	2	5	2
1986	Nd	Nd	0	**2001**	3	1	1
1987	Nd	Nd	1	**2002**	4	3	1
1988	Nd	Nd	1	**2003**	4	4	3
1989	Nd	Nd	0	**2004**	2	5	0
1990	0	2	1	**2005**	3	3	1
1991	0	0	0	**2006**	3	6	2
1992	0	0	0	**2007**	3	5	0

nd: no data
Source: Beck Online

c. Britain

Among the three early national systems, the British one has undergone the most radical transformation: what was once a consensual and informal national regulatory style has given way to a tougher, more legalistic approach to policymaking. A number of changes have been made, most of which began with the new British privacy law enacted in 1998.[99] First, in response to the widespread use of digital technologies and the increasing burden that registration has placed on administrative resources, the registration system has been cut back considerably so that it now applies only to a limited subset of personal data operations.[100]

Second, the Information Commissioner's Office, as the British privacy regulator is now known, has shed its ombudsman function. The administrative complaints procedure has been transformed into what is now called a "request for assessment": privacy victims are expected to come forward with evidence of the alleged violation and based on this evidence and any reply given by the wrongdoer, the Commissioner makes a determination of whether a breach of the Data Protection Act is likely or unlikely. Armed with this administrative determination, individuals are charged with vindicating

[99] Data Protection Act 1998.
[100] HEATHER ROWE, TOLLEY'S DATA PROTECTION ACT 1998: A PRACTICAL GUIDE 95-98 (2000).

their rights directly, before the recalcitrant corporation or government agency, and, if need be, in litigation before the courts. The onus, therefore, is now on the victim, not the Commissioner, to bring an end to private disputes. This new procedure also gives the Commissioner more discretion than in the past over whether to consider a complaint in the first place. This discretion is used to focus on those complaints that raise important matters of policy or systematic enforcement problems and, indeed, most complaints are dismissed before they get to the dispute resolution stage.[101] In sum, the administrative burden of amicably resolving privacy disputes has been dramatically reduced and the complaints procedure is now styled as a complement to agency policymaking and enforcement, similar to the French case.

Third, in 1998, the Information Commissioner obtained rulemaking powers for the first time. Although the privacy regulator had before used informal recommendations to assist industry with compliance, the new law expressly directs the Information Commissioner to advise the public on "good practice." Moreover, the Information Commissioner has obtained the power to promulgate rules ("codes of practice for guidance as to good practice") for different sectors and types of privacy issues. This is a more flexible mode of regulation compared to traditional administrative rules, *i.e.*, statutory instruments, but it nonetheless represents an improvement in the Commissioner's ability to set the terms of privacy protection. Today there are four official codes of practice, covering employment practices, telecommunications directory information, CCTVs, and internal corporate data-sharing. Furthermore, the Commissioner has been extremely active in formulating informal guidance and today there are thirty-four "good practice notes" and twenty-five "technical guidance notes" in force.[102] As with the reduction of registration, this expansion of rulemaking power has been driven by the proliferation of market actors and the belief that only with more specific regulatory standards, tailored to different types of data operations, is it possible to secure compliance among the many users of digital technologies.

Fourth, the Commisioner's enforcement powers have been improved. In 1998, to facilitate investigations, administrative subpoenas ("information notices") were added to the Commissioner's regulatory toolkit. Moreover, in a series of amendments enacted in 2008 and 2009, the Commissioner was given the power to conduct searches of government offices ("assessment notices") without a court warrant[103] and the power to impose administrative fines ("monetary penalty notices") for one important type of privacy violation—the intentional or reckless disclosure or obtaining of personal data.[104] Last, in contrast with the past when criminal penalties were limited to fines and low ones at that, custodial sentences are now available for one of the most common privacy crimes, the unlawful obtaining, buying, or selling of personal information.[105]

---

[101] *See* Faye Spencer, How the ICO deals with complaints, powerpoint presentation at the Data Protection Officers Conference 2009.
[102] *See* http://www.ico.gov.uk/Home/what_we_cover/data_protection/guidance.aspx (last visited March 1, 2010).
[103] Coroners and Justice Act § 173.
[104] Criminal Justice and Immigration Act 2008 § 144.
[105] *Id.* § 77.

It is unclear whether, in practice, the British privacy agency has moved towards a more punitive style of regulatory enforcement. For some of these enforcement powers, it is simply too early to tell. For those enforcement powers that are long-standing, either the data are not available (information notices) or they are erratic (search warrants and enforcement notices). However, beginning in 2004, when, as will be discussed below, the European Commission brought an enforcement action against Britain, the numbers have increased. Whether this trend will continue remains to be seen.

Britain—Administrative enforcement

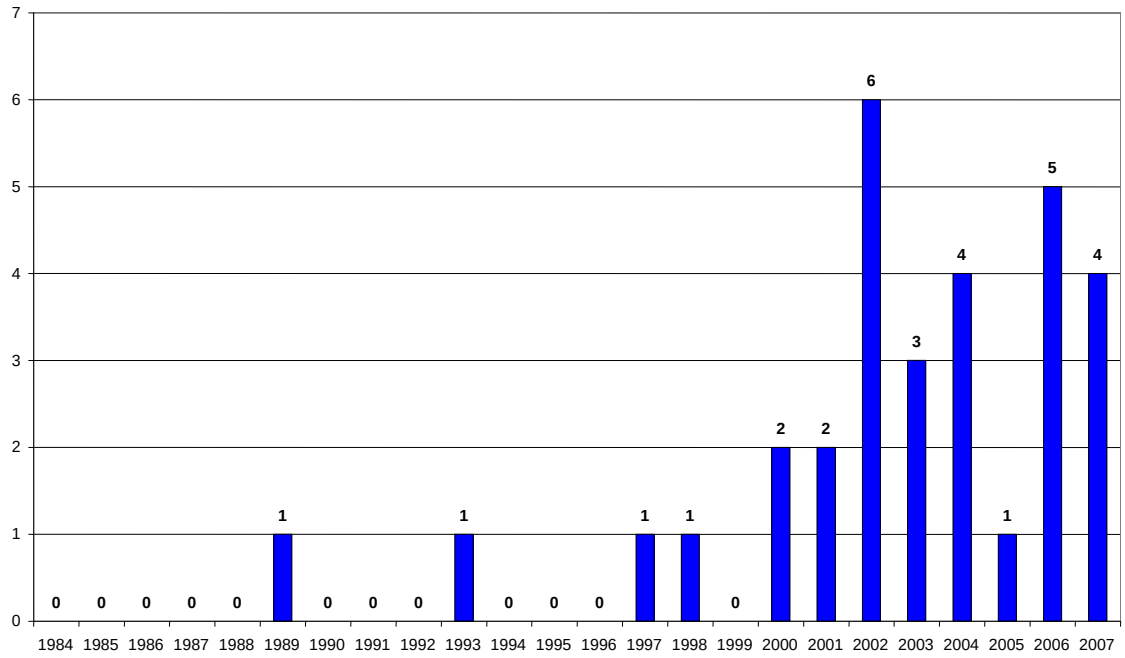
Year	Search Warrants	Enforcement Notices
2003/04	0	Nd
2004/05	6	3
2005/06	9	4
2006/07	12	7
2007/08	7	13
2008/09	14	9

Source: Information Commissioner's Office, Annual Reports and correspondence with Information Commissioner's Office

The fifth change made in the new privacy law was to expand litigation rights. While before individuals could sue for only four types of data privacy violations, the new law contains a general right of action, empowering individuals to sue for all statutory breaches. This change is reflected in litigation rates.[106] The graph below shows the number of cases alleging privacy violations that were decided by the High Court, one of the first instance courts with jurisdiction over privacy disputes and the only one whose decisions are consistently reported in the major electronic databases. Before 1989, my data set contains no cases and between 1989 and 1999, only four cases were litigated. But since 2000, plaintiffs have begun to raise data privacy claims more consistently. The numbers are still low but they have increased and they suggest that Britain is moving towards the norm for other European legal systems. In other words, as in France and Germany, individuals occasionally sue for privacy violations, but the threat of litigation remains quite remote and therefore administrative agencies still continue to bear primary responsibility for regulatory policy.

[106] As for administrative law litigation, it remains negligible. Only one case, dating to 2006, has ever been decided by the courts in the history of the British privacy agency and it involved not the private sector, but a dispute between the Information Commissioner's Office and the executive branch over a national security issue. *Secretary of State v. The Information Tribunal* [2006] EWHC 2958 (Admin).

High Court—Cases decided, 1984-2007



Source: Westlaw, UK-RPTS-ALL

Last, in what remains virtually the only element of continuity between contemporary and earlier regulatory practice, the Information Commissioner continues to promote industry self-regulation. As was described earlier, the Commissioner has championed two, related initiatives to encourage firms and government agencies to build privacy guarantees into their information systems and business practices—Privacy Impact Assessments and Privacy by Design. The Commissioner has invested considerable agency resources in promoting these self-regulatory tools, including extensive guidance materials and an ongoing series of workshops and seminars for corporate privacy officers.

The shift away from negotiated compliance towards rulemaking, agency enforcement, and some litigation was, in equal parts, a British response to the changing marketplace and a product of Europeanization. As early as 1990, British government officials agreed that registration should be eliminated and that the agency's rulemaking and enforcement powers should be enhanced.[107] Registration was seen as a regulatory burden, with no pay off in terms of privacy protection, and increasingly unsustainable in the face of the proliferation of market actors using digital technologies. Shortly thereafter the administrative dispute resolution system also came under fire as a resource-intensive,

[107] Review of the Data Protection Act: Report on Structure--The Home Office, 3 ENCYCLOPEDIA OF DATA PROTECTION, *supra* note 20 at 4824, 4840; Data Protection Act 1984: A Review by the Data Protection Registrar, Annual Report 1988/89.

ineffective device for achieving compliance.[108] This informal and individualized system of remedies was simply unable to keep pace with the widespread privacy violations occurring in the corporate (and government) world. What was needed, according to this line of thinking, was more precise standards and better enforcement tools, designed to deter breaches of these standards.[109] With the exception of strong enforcement powers, the British government embraced this reform program in the new 1998 privacy law. And even on enforcement powers, the government was eventually moved to action after it was confronted with dramatic evidence of serious privacy breaches occurring throughout the public and private sectors. As explained earlier, most of the Information Commissioner's new powers were introduced in 2008 and 2009, and this was in direct response to a string of politically embarrassing data privacy fiascoes—the loss of sensitive personal data on the approximately 25 million British citizens receiving child benefits, the use of data brokers to secretly vet employees, and more.[110]

Notwithstanding the domestic impetus for change, the legalistic, credible commitments dimension of Europeanization has also played a role in transforming the traditionally informal British regulatory process. In 2004, the European Commission opened an infringement procedure against Britain: the British privacy law did not include adequate inspection and fining powers, as required by the Directive.[111] In subsequent talks between the European Commission and the British regulator, the British regulator agreed to make better use of its existing investigation and sanctioning powers. And even though new enforcement powers have recently been enacted, the European Commission continues to exert pressure on Britain to show that these powers are adequate and are being used on a regular basis.

Furthermore, on the question of litigation rights, the historical record shows that Europeanization was *the* cause of change. In 1990, the British government had considered a right of action for all violations of the data privacy law but had rejected the proposal on the grounds that a general right of action could encourage "frivolous" claims, produce unlimited damages awards, and induce the privacy agency to adopt a more "confrontational approach," which was considered inferior to the existing "negotiated, consensual approach."[112] The British government was clearly afraid of stoking a regulatory culture akin to American adversarial legalism. But once the EU Directive was passed, the government no longer had any room for action, and had to create a general right of action to comply with the Directive's litigation provision. In essence, it was forced to alter the common law system of statutory torts, in which the legislative branch is firmly in control of what does and does not get litigated in the courts, to bring it into line with the civil law system, in which all breaches of regulatory statutes can potentially

[108] Data Protection Registrar, Consultation Paper on the EC Data Protection Directive (95/46/EC): Response of the Data Protection Registrar, July 1996 at 84-85 (on file with author).
[109] *Id.* at 46.
[110] *See* Commentary from the Information Commissioner's Office, 2nd Reading in the House of Lords, May 18, 2009.
[111] Peter Chapman, *Bolkenstein rebukes UK over lack of data privacy*, THE EUROPEAN VOICE, July 15, 2004.
[112] Review of the Data Protection Act: Report on Structure--The Home Office, 3 ENCYCLOPEDIA OF DATA PROTECTION, *supra* note 20 at 4824, 4835.

get litigated under the general tort provisions of the Civil Code. Today, the litigation issue is still alive: according to the European Commission, this British litigation right is too stingy to satisfy the requirements of the Directive. In the infringement proceeding just mentioned, the European Commission has alleged a number of shortcomings with the British data privacy tort: the courts should not require material damages to be proven before awarding damages for emotional distress; and the courts are allowed too much discretion in deciding whether to award injunctive relief such as the erasure or blocking of inaccurate personal data. It is too soon to tell whether the British government will budge on the issue, but if my earlier analysis of resistance to change on the institutional dimension of regulatory styles is correct, then we would expect the European Commission to be less successful on the litigation issue than on punitive agency enforcement.

d. Italy

Italy first enacted data privacy legislation in 1996.[113] As in Britain in 1984, the adoption of privacy regulation was externally driven. Italy wished to join the Schengen Agreement, an intra-European effort to cooperate on immigration and law enforcement which centered on a common database known as the Schengen Information System and due to come into force in 1995. To join, countries had to have data privacy legislation to ensure responsible use of the Schengen Information System. Without privacy legislation, Italy faced the prospect of being left outside of this European club, and therefore Italian policymakers sprang into action.

At the heart of the Italian regulatory scheme is an independent commission with extensive powers. As in France, the Italian privacy agency (*Garante per la protezione dei dati personali* or Garante) administers a registration and licensing system and wields related rulemaking powers. When the law was first passed, the registration requirement (*notificazione*) was near-universal, but, as in Britain and France, it soon became clear that this scheme created an unsustainable burden for regulators and digital-technology users alike. Therefore, by 2003, only those firms engaged in operations considered particularly hazardous, *e.g.*, databases on creditworthiness and genetic profiles, were required to register. Furthermore, administrative licenses (*autorizzazione*) are required for operations involving sensitive data such as race and for transfers of personal data to third countries that lack an adequate level of data protection. Operations, however, can be exempted from licensing based on administrative rules (*autorizzazione generale*) and since licensing, like notification, has proven to be extraordinarily burdensome, the Garante has made extensive use of this power.

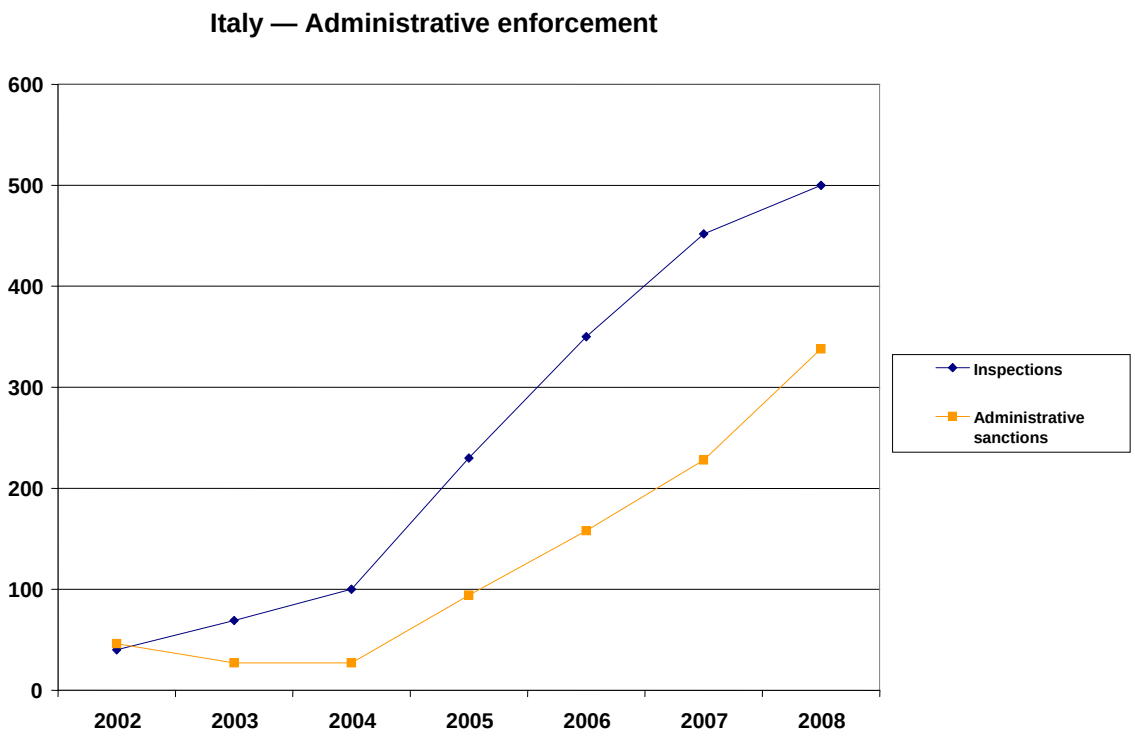
As elsewhere, self-regulation is used in the Italian system. Industry and professional associations are allowed to come forward with self-regulatory codes for official approval (*codici di deontologia e di buona condotta*) and they have done so in

[113] Legge 31 dicembre 1996, n. 675. The essential primer on the Italian law is GIOVANNI BUTTARELLI, BANCHE DATI E TUTELA DELLA RISERVATEZZA (1997). This account of the Italian framework is also based on the Garante's Annual Reports and interviews with Garante officials conducted on April 11, 13, & 14, 2003 and January 27, 2010.

considerable numbers. The Garante has approved more codes than any other regulator in this study: there are currently seven in force, one each for defense investigations, credit databases, personal data used for statistical and scientific purposes, the national statistics system, historical research, and journalists.

Turning to compliance, Italian regulators wield the full array of enforcement powers. There is an administrative subpoena power and an administrative inspection power, and the latter is more extreme than anywhere else: unlike France, Britain, and Germany, where a court order must be obtained before the police can be used to force entry, in Italy, the privacy agency can enlist the police directly, without a court application. Privacy violations can be punished with various sanctions: the regulator may order remedial measures, prohibit data processing operations, impose administrative fines, and refer offenses to the public prosecutor for a possible criminal action. Moreover, since the Italian law was first enacted, the administrative fining power has been improved a number of times, and therefore today the statutory maximums are much higher than they were originally and the types of privacy breaches that constitute administrative offenses are more extensive.

The practice of regulatory enforcement has been remarkably aggressive. Although the numbers were not consistently reported in the early years of the law, they were low overall since most of the Garante's resources were dedicated to educating the business community and disseminating information on data protection rights and duties. In recent years, however, the focus has shifted to enforcement and, as the graph below shows, the numbers on official agency inspections and administrative sanctions have exploded.



Source: Garante, Annual Reports

In a unique twist of the Italian scheme, the privacy agency also manages a system of administrative adjudication. This procedure mimics adjudication in a civil law court: once a complaint is filed, the Garante investigates the charge, hears the parties, decides the case, and affords a remedy to the victim with an administrative injunction. Italian administrative adjudication is considerably more formal and binding than the ombudsman dispute settlement that is practiced in Germany and that was characteristic of the early British scheme. It has also proven to be immensely popular, with more than 3,500 cases decided over the past ten years.

The last part of the Italian framework that speaks to regulatory styles is the system of statutory tort litigation. In Italy, the background rules on when individuals can sue for breaches of regulatory statutes are quite similar to German law. In the privacy law, these background rules were altered somewhat to make it easier to litigate: the same burden-shifting rule for proving fault that applies in cases involving ultra-hazardous activities was adopted and damages for emotional distress were made available across-the-board. However, as the table below demonstrates, Italian litigation rates in the court of last resort (Court of Cassation) remain low. In the courts of first instance (*tribunali*), litigation rates are erratic and considerably higher but even so, they are insignificant when compared to the enforcement and adjudication activities of the privacy agency.

Italy—Cases decided, 1996-2007

Year	First Instance	Court of Cassation		Year	First Instance	Court of Cassation
1996	0	0		**2002**	8	1
1997	0	0		**2003**	11	1
1998	0	0		**2004**	12	4
1999	5	0		**2005**	12	2
2000	3	1		**2006**	4	5
2001	3	1		**2007**	5	1

Source: Repertorio Foro Italiano, Giurisprudenza; Lex24 & Repertorio24; LexItalia.it

This Italian architecture is punitive while at the same time allowing for self-regulation and, overall, it is consistent with data privacy regulation elsewhere. Although the timing of the Italian law was driven by the Schengen Information System, the content was profoundly influenced by another European legal instrument, the EU Privacy Directive. The Italian law was drafted at the same time as the Directive was being negotiated, and therefore many provisions were lifted straight from the Directive, including registration and licensing, the extensive array of agency enforcement powers, and self-regulatory codes of conduct. In conjunction with pressure from the European network of privacy regulators, this legislative scheme has given rise to tough, deterrence-oriented enforcement tactics. Even though the Italian state, like France, is generally characterized as hostile to industry participation in policymaking, today, self-regulation is being used because of the policy diffusion process that occurred with industry codes of conduct. As in France and Britain, flexible registration and licensing have been cut back dramatically under the pressure of the ever-expanding digital marketplace. And tort litigation, as in the other country cases, is a minor component of the regulatory scheme.

VII. Beyond Privacy: Other Policy Areas

The pattern of European regulatory convergence experienced in the data privacy field is evident in a number of other policy areas too. In this section I briefly review legislation and secondary literature on consumer protection, anti-discrimination policy, and environmental protection, and I suggest that the same market and Europeanization forces have induced national regulators to adopt legalistic enforcement strategies and self-regulatory instruments in these areas too. Although far too broad a phenomenon to substantiate fully here, the claim is that tough administrative enforcement and self-regulation, set in a context of low judicial intervention, are emblematic of contemporary European regulatory styles.

The European Union has taken extensive action on consumer protection and making these consumer rights effective on the ground, in national regulatory systems, has always been a major source of concern. In the 1980s, the principal compliance strategy

promoted by the European Commission was consumer litigation.[114] But these efforts proved ineffective and therefore, by the late 1990s, the focus had shifted to regulatory enforcement and alternative dispute resolution.[115] The legislative output seeking to harmonize national regulatory styles has been formidable and the content largely mirrors the approach taken in the Privacy Directive: independent consumer agencies and extensive enforcement powers.[116] In addition, member states must give their consumers access to cheap, fast alternative dispute resolution, which in many national systems is handled by industry associations or individual firms and therefore represents a form of self-regulation.[117] Although the European Commission has put forward ambitious proposals to facilitate consumer and anti-trust litigation, they have been drastically cut back to accommodate hostile national governments and, therefore, any legislation that eventually passes will fall far short of American-style class actions.[118] A recent study on national regulatory systems suggests that these consumer protection initiatives have provoked a pattern of convergence similar to the data privacy case.[119] In Britain and the Netherlands, traditionally informal regulatory styles have given way to more legalistic compliance strategies, with the addition of independent consumer agencies and better enforcement powers. In sum, in consumer policy we observe the same mix of hard, legalistic enforcement, self-regulation, and resistance to tort litigation as in the data privacy case.

Anti-discrimination legislation in the European Union covers the whole gamut of suspect categories, from sex, to race, age, and more.[120] This legislation, like the Privacy Directive, seeks to promote the uniform enforcement of anti-discrimination rights with a standard set of national remedies and administrative powers. Similar to the privacy case, at the epicenter of this Europeanized regulatory template is a powerful, independent human rights agency. At the implementation phase, both the European Commission and the network of European human rights experts have put pressure on national governments to improve the independence and the powers of their human rights agencies, demonstrating that the credible commitments logic that I explored earlier is also at work in anti-discrimination policy.[121] Self-regulation is another component of this Europeanized regulatory template: the legislation encourages agreements between labor unions and employer associations, modeled after labor law in Scandinavia, Germany, and

---

[114] Directive 85/374 on Product Liability, art. 4, 1985 O.J. (L 210) 29; Directive 84/450 on Misleading Advertising, 1984 O.J. (L 250) 17.
[115] Interview with European Commission official, June 21, 2001.
[116] Directive 2006/114 on Misleading Advertising, art. 5, 2006 O.J. (L 376) 21; Directive 2005/29 on Unfair Business Practices, arts. 11, 13, 2005 O.J. (L 149) 22.
[117] *See, e.g.*, Directive 2008/48 on Credit Agreements, art. 24, 2008 O.J. (L 133) 66.
[118] European Commission, Green Paper on Consumer Collective Redress, Nov. 11, 2008, COM(2008) 794 final; European Commission, White Paper on Damages Actions for Breach of the EC Antitrust Rules, April 2, 2008, COM(2008) 165.
[119] Michel Faur et al., *Enforcement Practices for Breaches of Consumer Protection Legislation*, 20 LOY. CONSUMER L. REV. 361 (2008).
[120] Council Directive 2000/43, 2000 O.J. (L 180) 22; Council Directive 2000/78, 2000 O.J. (L 303) 16; Council Directive 2006/54, 2006 O.J. (L 204) 23.
[121] European Commission, Report on Implementation of Sex Discrimination Directive, July 29, 2009, COM(2009) 409 final, at 7; European Commission, Legal Seminar on Equal Opportunities and Anti-Discrimination, November 25, 2008, at 26-27.

elsewhere.[122] Last, American-style litigation was left out of the legislation. In what, by now, is a familiar sequence of events, the Commission sought to facilitate litigation on a broad scale by giving human rights groups standing to litigate discrimination cases without having to prove harm to individual victims, but the proposal was beaten back by national governments fearful of fomenting American adversarial legalism.[123] Thus in anti-discrimination policy too, the process of regulatory convergence has mimicked the dynamics of the privacy case.

Environmental protection is the last policy area to be considered here. Environmental protection is generally taken as a prime example of what has been called the "new governance" turn in EU policymaking. As documented by a number of scholars, the European Commission has come to champion a more flexible and participatory set of alternatives to classic command-and-control regulation. This has come in the shape of self-regulatory instruments such as private certification schemes, voluntary industry-government agreements, and information disclosure requirements.[124] Although the new governance literature generally does not explore their origins, most were first developed in countries like Britain and Germany with traditionally flexible regulatory styles and, later, were promoted by these same countries in the EU policymaking process.[125] In other words, the same diffusion mechanisms that led to the broad-based adoption of self-regulatory instruments in the privacy case have also been at work in environmental protection.

At the same time, EU policymakers have sought to address mounting frustration with uneven national compliance by forcing member states to adopt tougher regulatory sanctions. Although historically criminal law was off-limits to the European Union, criminal sanctions have recently been imposed for the scores of EU environmental laws that have been passed since the 1970s.[126] Moreover, a recent directive on environmental harm requires that national environmental agencies be equipped with extensive investigative and remedial powers, so that firms will be forced to clean up the environment and stop polluting.[127] Throughout the 1980s and 1990s the European Commission had favored a civil liability approach to environmental harm, which was openly modeled on American environmental law and entailed a significant role for private litigation in forcing polluters to comply.[128] Yet resistance from the member states was so great that the Commission moved to an agency-centered model, which is what eventually passed. This episode is yet another illustration of the difficulty of changing the institutional dimension of national regulatory styles and the European preference for administrative agencies over courts as a vehicle for policymaking and regulatory compliance. To conclude, in environmental protection as in data privacy,

---

[122] Directive 2000/43, art. 11; Directive 2000/78, art. 13; Directive 2006/54, art. 21.
[123] Interview with European Commission official, June 20, 2001.
[124] *See, e.g.*, Katarina Holzinger et al., *Governance in EU Environmental Policy*, in INNOVATIVE GOVERNANCE IN THE EUROPEAN UNION 45 (Ingeborg Tömmel & Amy Verdun 2009).
[125] *See, e.g.*, CHRISTOPH KNILL, THE EUROPEANISATION OF NATIONAL ADMINISTRATIONS 160-165 (2001) (private environmental certification).
[126] Directive 2008/99, 2008 O.J. (L 328) 28.
[127] Directive 2004/35 on Environmental Liability, 2004 O.J. (L 143) 56.
[128] Interview with European Commission official, January 28, 2010.

Europeanization does not appear to be generating a more litigious system but rather is forcing national regulators to create more space for self-regulation and to aggressively pursue those who break the law.

VIII. Conclusion

This study has demonstrated that European regulatory styles in the data privacy field are converging, not on adversarial litigation as anticipated in Americanization theory, but on a model of self-regulation and deterrence-oriented enforcement of government standards. In contrast with the past, when privacy compliance was achieved primarily through individualized and flexible forward-looking remedial measures, contemporary regulators are using the threat of inspections and sanctions to induce markets actors to take privacy standards seriously. France and Italy, traditionally hostile to industry involvement in policymaking, are now calling upon market actors to design and enforce more tailored privacy safeguards and Germany and Britain, where such self-regulation has always been common, are continuing to promote new self-regulatory techniques. This pattern of convergence has been driven by the regulatory realities of the new digital marketplace, as well as the credible commitments logic and the diffusion process triggered by Europeanization. Based on a review of three other policy areas, I suggest that this convergence phenomenon extends beyond the privacy case and is emerging throughout European regulatory governance.

Looking beyond European governance, these findings have implications for the study of convergence and transplants in comparative law more broadly. The American legal system is a highly salient model and it is generally regarded as a major source of legal export to the rest of the world, either because export is seen to be in the interests of the global hegemon or because, for various reasons, the American legal system is considered more advanced than others and therefore is thought to be the model towards which other countries will gravitate. However, as this study has shown, before concluding that foreign legal systems are being Americanized it is important to examine carefully the legal instruments that appear to be introducing American innovations and to gather data on how the law is being used on the ground. This empirical work is equally or more likely to find institutional resistance to change as it is to find Americanization. Theoretically, this resistance to change is a manifestation of the interconnected system of legal rules, judicial decisions, academic scholarship, and legal education that constitutes any legal order and that tends to insulate the legal establishment from dramatic transformation. The challenge for comparative research, therefore, is not simply to seek out American influence, but to understand the conditions under which domestic legal systems will accept or reject foreign legal innovation.

The second pitfall of the salience of the American model is that it can obscure other sources of legal transplants and convergence. In this study, northern legal systems and their self-regulatory legal instruments served as an important source of inspiration for southern European systems. Transplants at the regional level are likely to be extremely common, given the cultural and linguistic affinities that making legal borrowing attractive, and the extensive political and economic ties that bind together government

officials and lawyers within regions. Although the European Union is an extreme case of regional integration, other examples exist in Latin America, Asia, and Africa, and the dynamics of policy diffusion and legal borrowing in these regional settings deserve to be studied in their own right. The spread of American law through global markets and international organizations is certainly an important phenomenon, but it should be understood as one of a number of diffusion processes that intersects and combines with other, equally powerful, sources of domestic legal change.

Appendix: Note on Litigation Data

Two types of litigation were relevant to understanding the role of the courts in data privacy regulation: administrative law challenges to the decisions of national privacy agencies and tort suits brought against privacy violators under national data privacy laws. Below, I give the sources and methods that I used to collect data on each type of litigation.

Legal challenges to agency decisions

Britain: Annual reports

Italy: No source available.

Germany: No source available.

France: Lamyline database containing Council of State decisions since 1964. The Council of State has exclusive jurisdiction over challenges to CNIL decisions and therefore it was unnecessary to examine the decisions of the lower administrative courts. The case counts exclude cases involving disputes over access to police and national security files (indirect access cases) since the rule for allocating agency responsibility and court jurisdiction over these cases switched during the time period of interest and therefore the numbers before and after the rule change would not be comparable.

Statutory tort litigation

Research on tort litigation in Europe is handicapped by the lack of comprehensive reporting systems similar to the coverage of American courts that can be found in electronic databases like Westlaw and Lexis. However, in all four country cases, there is complete reporting of decisions rendered by the highest courts, and since litigants have an appeal of right to courts of last resort in the civil law systems of Italy, Germany, and France, the volume of cases decided by these courts is considerable. Moreover, for Italy, Germany, and the United Kingdom, I was able to obtain access to electronic databases with fairly good coverage of lower court decisions.

In all country cases, the initial searches were as broad as possible, based on the official title of the national law. Individual decisions were then excluded from the pool if it appeared from the text of the decision that the data privacy law did not serve as grounds for the lawsuit originally brought by the plaintiff in the court of first instance. These mainly included cases in which the data privacy law was used as a defense, *e.g.*, paternity suits seeking to obtain blood samples from alleged fathers, discovery orders, etc. Judicial decisions were also excluded from the data set if the data privacy law was referred to in passing but was tangential to the case and did not serve as grounds for the decision. Because case reports are so heavily edited in civil law countries, few cases were excluded on this basis in the French, Italian, and German searches. However, because judicial opinions are reported in full in common law systems, more hits were excluded on this basis from the British pool of cases.

The electronic databases used were as follows:

Great Britain: Westlaw, section “UK-RPTS-ALL”

France: LamyLine, “Jurisprudence de droit privé”; Dalloz.fr, “Jurisprudences”

Germany: Beck Online; Carl Heymanns Verlag, sections on BGHZ and BGHSt

Italy: Repertorio Foro Italiano, “Giurisprudenza”; Lex24 & Repertorio24; LexItalia.it