NELLCO
NELLCO Legal Scholarship Repository

Duke Law School Faculty Scholarship Series | Duke Law School

1-1-2007

European Versus American Liberty: A Comparative Privacy Analysis of Anti-Terrorism Data-Mining

Francesca Bignami
Duke University Law School

Follow this and additional works at: http://lsr.nellco.org/duke_fs

Recommended Citation
Bignami, Francesca, "European Versus American Liberty: A Comparative Privacy Analysis of Anti-Terrorism Data-Mining" (2007). *Duke Law School Faculty Scholarship Series.* Paper 75.
http://lsr.nellco.org/duke_fs/75

This Article is brought to you for free and open access by the Duke Law School at NELLCO Legal Scholarship Repository. It has been accepted for inclusion in Duke Law School Faculty Scholarship Series by an authorized administrator of NELLCO Legal Scholarship Repository. For more information, please contact tracy.thompson@nellco.org.

EUROPEAN VERSUS AMERICAN LIBERTY: A COMPARATIVE PRIVACY ANALYSIS OF ANTI-TERRORISM DATA-MINING

Francesca Bignami*

Forthcoming, Boston College Law Review, May 2007

ABSTRACT

The difference between European and American regulation of marketplace privacy is well-established: information privacy is protected more under European law than American law. Recently, with the revelation of a number of U.S. government, anti-terrorism programs, it has become clear that the transatlantic difference is not limited to the market. Also in the face of government action, Europeans protect information privacy more than Americans. This paper brings to light the legal differences between the two systems by considering the case—real in the United States, hypothetical in Europe—of a spy agency's database of call records, created for the purpose of identifying potential terrorists. The paper explains that, under American law, such an anti-terrorism database might very well be legal, and that, under European law, such an anti-terrorism database would clearly be illegal. It then reviews the barriers to transatlantic cooperation on fighting terrorism that have been created by the legal difference. The paper also considers the reasons for this transatlantic difference—surprising in view of the common wisdom that Americans are more suspicious of government interferences with individual liberty than Europeans. The paper concludes with a few recommendations for the reform of American information privacy law, principal among them being the establishment of an independent privacy agency.

INTRODUCTION

On April 9, 1940, the Nazis occupied Norway. In May 1944, seeking to bolster the German army in the face of the mounting Allied offensive, the Nazis decided to conscript Norwegian men of fighting age into the army.[1] Men born in three different years were to be sent to the Eastern Front. For this purpose, Norwegian government files containing names, addresses, the sex, dates of birth, and other personal information on the population were to be used. When the Norwegian resistance learned of the plan, they attempted to destroy the files, unsuccessfully. So the resistance fighters turned to machines that were to be used to sort, by age cohort, the files—only two of which existed

---

* Professor, Duke University School of Law. Many thanks to the Americans and Europeans who assisted me with this project: Jon Bing, Erwin Chemerinsky, Alexander Dix, Christopher Docksey, Patrick Doelle, David Fontana, Anna-Mirjam Frey, Carl Lebeck, Xavier Lewis, Joan Magat, Noah Novogrodsky, Giorgio Resta, Marc Rotenberg, Spiros Simitis, Daniel Solove, Graham Sutton, Stefan Walz, and David Zaring.

[1] *See* Jon Bing, *in* ANGELL 2002 114-23 (Lill Granrud, Johan Fredrik Grøgard, Per Quale, Jan Erik Vold eds., 2002).

in Norway. They destroyed both. Without the ability to tabulate the population data, a Norwegian draft was too difficult to put into effect and the Nazi plan had to be dropped.

This story and countless others, with less-happy endings, underpin the law of information privacy in Europe today. The dangers of any large-scale government effort to collect, catalogue, and manipulate information on individuals are never far-fetched. Preventing them is the object of European privacy law.

Americans have never suffered the same disastrous abuses of their personal records as did Europeans during World War II. Perhaps that is why American law is so much more complacent than European law in the face of massive government databases of personal records. One recent illustration of this transatlantic difference is the revelation, in May 2006, of a National Security Agency (NSA) database with the phone records of millions of ordinary American citizens. Ever since September 11, the NSA has been receiving the call records of at least one major telecommunications provider for purposes of an anti-terrorism data-mining program. Even though the discovery provoked public uproar, whether the law was broken is entirely unclear. In most European countries, had such a data-mining program come to light, the outrage would have been not only political but also legal: the spy agency would be acting in flagrant disregard of the law.

In Europe, such a program would have to be authorized by a *public* law or regulation. It would have to be reviewed, in advance, by an independent privacy agency. Even though a European spy agency might be permitted access to the same type of call data, it would not be allowed to store the data for as long as the NSA has—over five years now. The data could be mined only for certain statutorily prescribed "serious" threats. It could be passed on to law enforcement agencies only if a certain factual threshold had been met for suspecting an individual of having committed, or planning to commit, one of those serious offenses. The same independent agency would have enforcement and oversight powers, to guarantee that the program was being run in accordance with the law. Individuals would have a right—albeit subject to numerous exceptions—to check on their personal data, to ensure that it was being used lawfully.

This article explores the European law of data protection and explains why a government data-mining program like the NSA's would fall afoul of that law. (In Europe, information privacy is known as "data protection.") The comparative exercise serves many purposes. By taking the same set of facts and comparing how those facts would fare in two different legal systems—American and European—the differences between their laws are brought into sharp focus. Considering a concrete set of facts is especially valuable in this area of the law because many European data-protection rules are framed in such abstract terms that it is difficult to appreciate how, in the hands of regulators and courts, they serve to curb government action.

Beyond description, this comparison has far-reaching ramifications for transatlantic cooperation on fighting crime and protecting national security. This article draws out the many points of difference between information-privacy law in Europe and

the United States. Because of the difference, European authorities are prohibited, by law, from sharing intelligence on a routine basis with their American counterparts. Only an agreement between Europe and the United States, under which the United States commits to an equivalent level of data protection, can overcome the legal barrier to information exchange. And to date, it has been impossible to reach such an agreement. Not only has transatlantic cooperation been stymied, but predictions of regulatory convergence between Europe and the United States have failed, quite spectacularly, in this area. Conflicts between regulatory systems have not resulted in convergence but rather have been resolved through ordinary territoriality principles: when the territory or resources to which access is sought is American, American rules prevail; when it is European, European rules prevail.

The last aim of this comparison is to encourage critical reflection on American law. When it comes to information privacy, liberty is protected more in Europe than in the United States. This observation goes against the grain of recent privacy scholarship: in that view, American privacy law protects individual liberty against the state while European privacy law promotes dignity in inter-personal relations. But as this analysis will demonstrate, privacy law in Europe also protects liberty and, in the context of anti-terrorism data-mining, does so more than American law. The difference is even more striking in light of the near-identical statutes adopted on both sides of the Atlantic in the early 1970s—a single regulatory solution to what, at the time, was considered to be a common policy problem of protecting individual privacy in the age of information technology. A number of factors have contributed to this progressive divergence: the absence of an agency committed to privacy policy in the American regulatory scheme, the rise of executive power in the United States at the very same time that national executives in Europe are being checked, more and more, by the law of multiple Europe-wide political communities, and the influence of the Nazi experience on contemporary European human rights law.

By expanding the realm of legal possibilities, comparison can serve as an impetus for legal change at home. Wholesale borrowing from Europe would be misguided: a full-fledged constitutional right to information privacy and a cross-cutting law regulating information privacy in both the private and public sectors would be unlikely to achieve the desired result of curbing government data-mining. Rather, this article recommends a number of changes to the U.S. Privacy Act of 1974. Although the intent of the drafters was to curb information privacy abuses by government actors, across-the-board, the recent experience with data-mining programs demonstrates that the original ambition has been disappointed. Amending the Privacy Act would increase the transparency of data-mining, enhance the public debate on the privacy costs of government programs, place some fairly modest limits on the government's uses of personal data, and improve oversight and enforcement. The European experience sheds light on what, in the original transatlantic regulatory scheme, has worked well and deserves—once again—to become part of American privacy law.

The rest of this article is organized as follows: In the first part, the NSA call database is described in more detail. This is followed by an overview of three sets of

legal categories that are relevant, albeit in different permutations, to the analysis on both sides of the Atlantic. The third part considers the applicable U.S. constitutional and statutory law and concludes that the President might very well have lawfully authorized the database. The fourth part sets out the European law that would apply to that same data-mining program, conducted by a European spy agency, and reveals how the program would come into conflict with the law. In the last part, the consequences of the comparison are explored, both for transatlantic relations and for understanding American privacy law.

I. THE NSA CALL-RECORDS PROGRAM

These are the details of the NSA call-records program that have been revealed so far.[2] Immediately following the terrorist attacks of September 11, the NSA approached the country's major telecommunications carriers, asking them to hand over their customers' calling records and to update those records periodically. The NSA sought information on all calls made and received: to whom, from whom, when, and for how long. Customers were identified only by their phone numbers, not by their names, but a quick search of any public directory readily matches the phone number with the name. AT&T, the largest American telecommunications company, complied with the request. So did Verizon's subsidiary MCI. Qwest did not. And, after some confusion in the media, it appears that neither did BellSouth. But even with just AT&T and Verizon cooperating, the database most likely contains information on tens of millions of Americans.

The NSA has been "mining" the database to identify possible terrorists. Databases can be put to many different uses. Most simply, a database can organize large amounts of information so that, at a later time, that information can be retrieved easily. Statistical software can be applied to the data in the system. Data-mining is probably one of the most sophisticated, technologically speaking, of the possible uses of data. In the words of one helpful explanation for non-specialists

> Many simpler analytical tools utilize a verification-based approach, where the user develops a hypothesis and then tests the data to prove or disprove the hypothesis. For example, a user might hypothesize that a customer who buys a hammer, will also buy a box of nails. The effectiveness of this approach can be limited by the creativity of the user to develop various hypotheses, as well as the structure of the software being used. In contrast, data-mining utilizes a discovery approach, in which algorithms

[2] USA Today has done most of the reporting on this story. The facts recounted here are drawn largely from USA Today's original article of May 11, 2006 and its follow up article of June 30, 2006: Leslie Cauley, *NSA has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2001, A1 and Susan Page, *Lawmakers: NSA Database Incomplete*, USA TODAY, June 30, 2006, A1. Some more description of the NSA program can be found in *Terkel v. AT& T Corp*., 2006 WL 2088202 (N.D. Ill. July 25, 2006) and Letter from Electronic Privacy Information Center to Federal Communications Commission seeking investigation of telephone companies in connection with disclosures to the National Security Agency (May 17, 2006), http:// www.epic.org/privacy/phone/fcc-letter5-06.html.

> can be used to examine several multidimentional data relationships simultaneously, identifying those that are unique or frequently represented. For example, a hardware store may compare their customers' tools purchases with home ownership, type of automobile driven, age, occupation, income and/or distance between residence and the store. As a result of its complex capabilities, two precursors are important for a successful data-mining exercise; a clear formulation of the problem to be solved, and access to the relevant data.[3]

For the hardware store, the problem is picking out those consumers likely to buy hammers and nails. For the Department of Health and Human Services it is detecting welfare fraud. And for the NSA, it is spotting likely terrorists.

Mining the data is only one part of the process. The data must first be collected, generally in many different databases. It must then be cleaned, to improve the quality of the data. This can

> involve the removal of duplicate records, normalizing the values used to represent information in the database (e.g., ensuring that "no" is represented as a 0 throughout the database, and not sometimes as a 0, sometimes as a N, etc.), accounting for missing data points (e.g., an individual whose age is shown as 142 years), and standardizing data formats (e.g., changing dates so they all include MM/DD/YYYY).[4]

Care must be taken to render different databases and data-mining software interoperable. Only then can data-mining be expected to generate valid results.[5]

How the call records are being mined by the NSA is unclear. According to some reports, only calls involving known or suspected al Qaeda affiliates are targeted.[6] By analyzing their call records, the NSA can gain insight into their activities, learn of possible terrorist plots, and identify other individuals who might be collaborating with al Qaeda. The possibility, however, that more general criteria are being used to mine the data has not been ruled out. For instance, the NSA might analyze phone numbers with calls to or from the Middle East and located in geographic areas known to be Muslim communities. What happens afterwards with the phone numbers identified as likely terrorist numbers is unclear, too. One possibility is that the information is used by the NSA or other government agencies to undertake more intrusive surveillance, for instance, eavesdropping on phone lines. Another possibility is that the pool of suspects is further

---

[3] Jeffrey W. Seifert, *Data-mining and Homeland Security: An Overview*, Congressional Research Service Report for Congress 2 (Jan. 27, 2006).
[4] *Id.* at 17.
[5] *Id.* at 2, 17-18.
[6] *See* Susan Page, *Lawmakers: NSA Database Incomplete*, USA Today, June 30, 2006, A1. *Lawmakers: NSA Database Incomplete*, USA TODAY, June 30, 2006.

narrowed by matching the suspicious phone numbers with other records such as credit-card histories, financial information, and airline-passenger records. Given the secretive nature of the database these are, at best, informed guesses; the NSA's data-mining methods are unlikely to be revealed anytime soon.

This is just one of many anti-terrorism data-mining initiatives that have come to light since September 11.[7] The most notorious is Total Information Awareness, later renamed "Terrorism Information Awareness" in response to public criticism and ultimately de-funded by Congress. The goal of Total Information Awareness was to combine all electronic information available on individuals—like internet purchases, airline passenger data, and driver records—to single out terrorism suspects.[8] Others include the Computer-Assisted Passenger Prescreening System (CAPPS II), now called Secure Flight and designed to match airline-passenger records with other data in order to stop likely terrorists from boarding airplanes. The Multistate Anti-Terrorism Information Exchange (MATRIX) Pilot Project, which seeks to combine information from a variety of databases, including state law enforcement records, to assist with criminal investigations. And the Department of the Treasury's acquisition, for data-mining purposes, of all records on international money transfers held by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).[9] In the interest of brevity and clarity, the comparative legal analysis in this article focuses on a call-records program undertaken by a spy agency. But the analysis is also relevant to the many other anti-terrorism data-mining programs that have surfaced in the past couple of years. To be sure, the statutory and constitutional specifics differ, especially in the United States, but the fundamental principles of the two legal systems and their points of contrast remain the same.

Based on what legal authority did the NSA embark on its data-mining mission? The agency was created by a secret executive memorandum in 1952.[10] It was to be the sole foreign intelligence agency responsible for intercepting communications, what is generally called signals intelligence in contrast to human intelligence. The NSA was placed under the organizational umbrella of the Department of Defense. In the years since 1952, the NSA has become a critical element of the intelligence community. It has extraordinarily powerful and sophisticated computing facilities, with the capacity to intercept and analyze any type of communication, anywhere in the world. The NSA is

---

[7] *See* Seifert, *Data-mining and Homeland Security*, *supra* note__at 5-17.

[8] *See* DANIEL J. SOLOVE, MARC ROTENBERG & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 604-05(2d ed. 2006).

[9] Eric Lichtblau & James Risen, Bank Data Sifted in Secret by U.S. to Block Terror, NY TIMES, June 23, 2006, A1.

[10] PATRICK RADDEN KEEFE, CHATTER: DISPATCHES FROM THE SECRET WORLD OF GLOBAL EAVESDROPPING 7 (2005). The agency's original mandate was considerably elaborated and extended in Executive Order 12,333, promulgated by President Reagan in 1981. *See* 46 Fed. Reg. 59,941, pt. 1.12(b) (Dec. 4, 1981). While Congress has never enacted a specific enabling statute for the agency, it has acknowledged the agency through appropriations legislation and laws directed at the NSA. *See, e.g.*, National Security Agency Act of 1959, Pub. L. No. 86-36, 73 Stat. 64, codified at 50 U.S.C. § 402 note; *see also* Peter E. Quint, *The Separation of Powers under Carter*, 62 TEX. L. REV. 785, 875n.478 (1984).

the agency responsible for some of today's most notorious spy programs: Echelon,[11] warrantless wiretapping of international phone calls,[12] and, of course, the call database.

Originally, the NSA was exempted from all regulation curbing the government's intelligence activities.[13] In the aftermath of Watergate, however, Congress enacted legislation specifically targeted at the NSA's intelligence-gathering—the Foreign Intelligence Surveillance Act. Later, in Executive Order 12,888, President Reagan set down surveillance guidelines for the entire intelligence community including the NSA. Some of these restrictions are explored below. As we will see, however, they are largely ineffective against the collection and use of personal data that does not entail the interception of wire or electronic communications.

As for the call-records program, it was most likely authorized by a secret presidential directive. The President has not yet spelled out the legal grounds for the directive but they are likely to be similar to those advanced in support of the warrantless wiretapping program uncovered in December 2005.[14] In a White Paper submitted to Congress, the administration made two legal arguments in support of warrantless wiretapping: it was a lawful exercise of the President's constitutional powers under Article II and it was authorized by the Authorization for Use of Military Force (AUMF), enacted by Congress in the immediate aftermath of September 11.[15] According to the administration, the President's constitutional duty to serve as Commander-in-Chief of the Armed Forces and to prevent armed attacks against the nation includes the power to conduct warrantless surveillance within the United States for foreign intelligence purposes.[16] In the AUMF, Congress authorized the President "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorists attacks" of September 11 in order to prevent "any future acts of international terrorism against the United States." The administration maintains that Congress intended for the statute to cover domestic electronic surveillance, not only conventional military operations: such activity is necessary to identify the enemy and to foil future terrorist attacks.[17] Both of these

---

[11] Lawrence D. Sloan, *Echelon and the Legal Restraints on Signal Intelligence: A Need for Reevaluation*, 50 DUKE L. J. 1467 (2001).

[12] David Cole & Martin S. Lederman, *The National Security Agency's Spying Program: Framing the Debate*, 81 INDIANA L. J. 1355 (2006).

[13] *See* Michael V. Hayden, *Balancing Security and Liberty: The Challenge of Sharing Foreign Signals Intelligence*, 19 NOTRE DAME J. L. ETHICS & PUB POL'Y 247 (2005) (describing the principal statutes and executive orders applicable to the NSA); Robert N. Davis, *Striking the Balance: National Security vs. Civil Liberties*, 29 BROOK. J. INT'L L. 175 (2003) (same).

[14] In July 2006, Michael Hayden, Director of the NSA at the time that the call database was created, was confirmed by the Senate for the position of Director of the CIA. In his confirmation hearings, he was asked about the legality of the call database. Hayden said that the program was vetted by the NSA's General Counsel and the Inspector General and that both had said that the program was within the President's Article II powers. Hayden, however, did not recollect any discussion of the Authorization for the Use of Military Force.

[15] *Legal Authorities Supporting the Activities of the National Security Agency Described by the President*, 81 IND. L. J. 1374 (2006).

[16] *Id.* at 1380.

[17] *Id.* at 1384-85.

arguments can also be made in support of the call database: by ordering the creation of the call database, the President furthered his constitutional duty to protect national security and took the steps necessary to prevent "any future acts of international terrorism," as instructed by Congress in the AUMF.

Since the discovery of the call-records program, a number of lawsuits have been filed in federal court against the telecommunications providers and the government.[18] In addition, complaints against the providers have been filed with telecommunications regulators in over twenty states.[19] The telecommunications companies and the government, however, have already successfully defended in two of these cases based on the state secrets privilege.[20] This privilege protects information related to national security from disclosure because of the possible harm to national defense and to the success of future intelligence-gathering operations. In the two cases in which the courts have found in favor of the privilege, the plaintiffs' claims had to be dismissed because without court-ordered discovery it would be impossible for them to prove any of their claims. Thus, it might very well be that, as a result of the state secrets privilege, the lawfulness of the call-records program will never be decided by the courts.

II. SOME INITIAL TRANSATLANTIC COMPARISONS

How convincing is the President's legal defense of the NSA call database? As we shall see, plausible. But before launching into a detailed discussion of the legal framework, a couple of distinctions, important to the analysis on both sides of the Atlantic, should be borne in mind. The first is the difference between the content of communications and the incidents of communications—like who was called, when, and for how long. This is significant for examining the government's interference with privacy in the United States, considerably less so in Europe. In the United States, the content of, say, a telephone call or an email message is extensively protected under constitutional and statutory law, but the incidents are not, especially when gathered after the communication has occurred. In Europe, the collection of both types of data is considered an interference with the fundamental right to privacy. Even in Europe, however, government surveillance is generally considered more intrusive in the case of content data and therefore more difficult to justify in the face of a legal challenge.

The second distinction is the one drawn between communications data and all types of personal data. Because letters, phone conversations, emails and other types of communications are believed to be more revealing of one's self than a decision to purchase a book on the internet, for example, the government's ability to obtain that kind of personal data is covered by separate, more stringent regulation on both sides of the

---

[18] *See In re* National Security Agency Telecommunications Records Litigation, 444 F. Supp.2d 1332 (Jud. Pan. Multi. Lit. 2006).

[19] ACLU, Formal Complaint and Request for Investigation of AT&T and Verizon 2, filed with Michigan Public Service Commission, July 26, 2006, available at http://www.aclumich.org/pdf/publicserviceletter.pdf.

[20] *See* ACLU v. NSA, 438 F. Supp.2d 754, 765-66 (E.D. Mich. 2006); Terkel v. AT&T, 441 F.Supp.2d 899 (N.D. Ill. 2006).

Atlantic. Where Europe and the United States part ways is on their treatment of "all types of personal data." With respect to personal data processing by government actors, the U.S. legal framework is far less demanding than the European one. As for the private sector, an all-encompassing category for "all types of personal data" does not exist in the United States. Rather, uses of *specific* types of personal data are regulated—health information, video-store records, financial information, and so on.[21] By contrast, in European law all personal data processing is treated as potentially problematic, even when undertaken by private actors.

The last important distinction regards not the type of personal data collected, but the government purposes for which it is collected. The law in both the United States and Europe treats information-gathering for purposes of law enforcement differently from information-gathering for purposes of protecting national security. The former is regulated more stringently than the latter because of the different aims and consequences of the two types of government activities.[22] Criminal investigations are relatively narrow in scope—their focus is a specific past, or imminent future, event. By contrast, agencies charged with protecting national security must monitor a wide, inchoate range of individuals and activities that might, sometime in the future, threaten the well-being of the population. Furthermore, the purpose of a criminal investigation is to prosecute and convict individuals, with draconian consequences for their life and liberty interests. By contrast, criminal prosecutions are tangential to what national security agencies do. They do not have arrest powers but instead must refer cases to the police if a plot is so far advanced that arrest and prosecution are warranted. Rather, the mission of such agencies is to thwart the most dangerous types of threats—often turning a blind eye to routine crime—and to do so using a variety of tactics. The targets of national security surveillance, therefore, are not as likely to be detained and imprisoned as are those of police investigations. Their rights are clearly compromised, but not as directly as with criminal investigations.

Again, Europe and the United States differ as to how they further parse the categories. On the national security side, European legal systems are designed to ward off two types of threats: domestic and foreign. One agency is responsible for gathering intelligence abroad on threats posed by foreign governments—in the old days the Soviet Union. Another agency is charged with gathering intelligence at home, on activities sponsored by foreign powers (counter-intelligence) as well as on home-grown security threats.[23] In the past those home-grown threats came from extremist and separatist

---

[21] The government's use of many of these same types of personal data is also afforded special regulatory treatment. *See, e.g.*, The Right to Financial Privacy Act, Pub. L. No. 95-630 (1978), codified at 29 U.S.C. §§ 3401-3422; Fair Credit Report Act, Pub. L. No. 90-321 (1970), codified at 15 U.S.C. § 1681.

[22] *See generally* RICHARD A. POSNER, PREVENTING SURPRISE ATTACKS: PREVENTING TERRORISM REFORM IN THE WAKE OF 9/11 (2006) (describing difference between law enforcement and national security functions).

[23] In Germany, there are two main sets of national security agencies: the Office for the Protection of the Constitution (Bundesamt fur Verfassungschutz or BfV) and the BfV's counterparts at the Land (state) level, responsible for domestic intelligence; and the Federal Intelligence Service (Bundesnachrichtendienst or BND), responsible for foreign intelligence. *See* Shlomo Shpiro, *Parliamentary and Administrative Reforms in the Control of Intelligence Services in the European Union*, 4 COLUM. J. EUR. L. 545, 550-51 (1998); *see*

terrorist groups like the Bader Meinhof and the Irish Republican Army; today they include radical Islam terrorist cells. Both sets of agencies operate under far less cumbersome procedural guidelines than do the police. Oversight is generally entrusted not to the judiciary but to the legislative and executive branches. Specifically, both sets of agencies are covered by the more permissive surveillance regimes that will be discussed in the section on European law—permissive, that is, compared to police surveillance for purposes of criminal prosecutions.

By contrast, in the United States, national security is conceived mostly as security from foreign powers abroad, not from internal threats and especially not from home-grown internal threats. On the bureaucratic level, there are no domestic counterparts to the country's foreign intelligence agencies—the Central Intelligence Agency (CIA) for human intelligence and the NSA for signals intelligence. The Federal Bureau of Investigation (FBI) is charged with *both* criminal investigations of violations of federal law and domestic intelligence operations. Those domestic operations, moreover, are directed against activities sponsored by foreign governments or groups, not by domestic ones. The rules for national security surveillance, set down in the Foreign Intelligence Surveillance Act of 1978 (FISA), are largely responsible for this institutional state of affairs.[24] As the name suggests, the statute applies only when the government seeks to obtain foreign—not domestic—intelligence within the United States: its rules are triggered when the target of the investigation is a "foreign power" or an "agent of a foreign power."[25]

In fact, until recently, the FBI's paradigm for both domestic intelligence operations and criminal investigations has been the more rights-abiding law enforcement one, not the national security one.[26] This is the product of the organizational culture that developed in the 1970s in response to congressional investigations into the FBI's secret surveillance of civil rights leaders and other political activists. As Jacqueline Ross explains, under the FBI guidelines crafted in the 1970s for domestic security investigations:

> the FBI was to restrict domestic intelligence operations to the investigation of individuals or groups who not only violate civil rights or seek to interfere with or overthrow the government, but who do so through

---

also FRANÇOIS THUILLIER, L'EUROPE DU SECRET: MYTHES ET RÉALITÉ DU RESEIGNEMENT POLITIQUE INTERNE 18 (2000). The structure of the security services in France is even more complicated. Intelligence on home-grown security threats is handled by a department of the National Police, the Direction centrale des renseignements généraux (DCRG). There is also an anti-terrorist section of the National Police: the Division nationale anti-terroriste (DNAT). It is responsible for investigating and preventing all terrorist activities in France. Domestic intelligence on security threats encouraged by foreign powers is handled by the Direction de la Surveillance du Territoire (DST). *See id.* at 112-13. The Direction générale de la securité extérieure (DGSE) is France's classic spy agency, responsible for gathering signals and human intelligence *outside* France. *See id.* at 185.

[24] *See* Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, codified at 50 U.S.C. §§ 1801-1811.

[25] 50 U.S.C. § 1804(a).

[26] *See* Jacqueline Ross, The Elusive Line Between Prevention and Detection of Crime in German Undercover Investigations 36 (paper on file with author).

> activities that "involve or will involve the violation of federal law" as well as "the use of force or violence." Thus the standard for proper covert operations in the intelligence arena became the criminal standard—requiring some indication that criminal offenses were in the offing.[27]

Compared to Europe, more government investigations are regulated as policing than as defending against national security threats. This is true even today, even after all the revisions that have been made since September 11 to the FBI guidelines and FISA.[28]

The Nixon-era reluctance to allow national security operations to be directed against primarily domestic conspiracies also makes sense of a fundamental anomaly, at least in European eyes, of the NSA call database: why is a program involving primarily individuals within the United States being handled by an agency created to gather foreign signals intelligence? For most of the calls, even the suspicious ones, involve individuals living in the United States whose formal ties to the United States are likely to be at least as strong as, if not stronger than, their ties to a foreign organization. In other words, the threat that one might hope to discover with such data-mining is as likely to be a threat coming from fundamentalist Islam groups established inside the country, as from al Qaeda operatives abroad. The answer to this puzzle is that the architecture of the legal system does not fully contemplate such investigations. In a place like Germany, France, or the United Kingdom, with one or more domestic security agencies, such a program would be handled by one of those bodies. But in the United States, the NSA was the only viable institutional candidate.

III. THE UNITED STATES: LEGAL PLAUSIBILITY

Now for a detailed consideration of the law on the American side of the Atlantic. First, the constitutional law. The Fourth Amendment, generally the first line of defense against intrusive surveillance, does not apply in cases like the NSA call database. Under the Supreme Court's case law, a person must have a reasonable expectation of privacy before the Fourth Amendment's prohibition on unreasonable searches and seizures and the related warrant requirement will apply. In *Katz v. United States*,[29] the Court held that individuals have a reasonable expectation of privacy in the content of their telephone conversations. But, over a decade later, the Court held that individuals do not have a reasonable expectation of privacy in the numbers dialed from their telephones.[30] Why? According to the Court, individuals know that the numbers dialed from their lines can be recorded by their providers and that, indeed, these numbers are routinely recorded for legitimate business purposes such as billing. Because callers know of this exposure to third parties, the Court reasoned, they cannot expect for their dialing information to

---

[27] *Id.* at 36.
[28] *Id.* at 37. For a description of the changes to FISA made by the USA PATRIOT Act and the reauthorization of the USA PATRIOT Act, see SOLOVE, ROTENBERG & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note__ at 288-309.
[29] 389 U.S. 347 (1967).
[30] *Smith v. Maryland*, 442 U.S. 735 (1979).

remain secret. In making telephone calls and doing business with telephone companies, subscribers "assume the risk" that their records will be exposed to others, including the police.[31]

This case law is the source of the distinction between content and non-content or "envelope" communications data.[32] What is written in a letter—today, an email—and what is said in a telephone conversation is considered private. Warrantless government intrusions are believed to be obnoxious. By contrast, individuals cannot claim a privacy interest in those identifiers that are necessary for the communication to occur—the mailing address, the routing information, and the telephone numbers. That information is too "prosaic" for a constitutional privacy right to attach.[33] Because the call records collected by the NSA fall into the non-content category, they are not covered by the Fourth Amendment.

Nor would such information be protected under the Supreme Court's substantive due process doctrine. The Supreme Court has long recognized that certain types of personal decisions are constitutionally protected from government inference, as part of the right to "liberty," even though they are not specifically listed in the Bill of Rights. The most notorious of these personal decisions, of course, is abortion.

In 1977, the Court suggested that personal information might also be constitutionally protected as a liberty interest. In *Whalen v. Roe*, the Court considered a challenge to a New York statute requiring physicians to report to the state Department of Health all prescriptions written for drugs with both medical and recreational uses—drugs like opium, cocaine, and marijuana.[34] The Court rejected the challenge, but not before elaborating on the harm that disclosure of such medical information might cause patients and reviewing the various safeguards in place to prevent disclosure except when necessary to stop illegal drug abuse. Since *Whalen*, however, the Supreme Court has been silent on the so-called "constitutional right to information privacy" and the federal circuits have come down differently on the very existence, as well as the contours, of the right.[35] Even setting aside this uncertainty, information on one's phone calls would most likely not count as part of such a right. The Fourth Amendment case law on the lack of a reasonable expectation of privacy is especially damning on this point. In sum, even if there were an established right to information privacy, it is highly unlikely that call data would be covered by the right, and even if it were covered, that the security measures in place to protect against unwarranted disclosures were so deficient as to render the NSA database unconstitutional.

---

[31] The assumption of the risk rationale was first used by the Supreme Court to deny Fourth Amendment protection to customer account information held by banks. *See* United States v. Miller, 425 U.S. 435 (1976).

[32] *See* Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 611 (2003); Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264 (2003-2004).

[33] *Smith v. Maryland*, 442 U.S at 748 (Stewart, J., dissenting).

[34] 429 U.S. 589 (1977).

[35] *See* SOLOVE, ROTENBERG & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note__ at 400-402.

Some of the lacunae in the Supreme Court's case law have been filled by legislative enactments. Even though, therefore, the incidents of communications are not constitutionally shielded from government scrutiny, they do receive some protection under statute—albeit less than the contents of communications. Surveillance conducted for law enforcement is regulated separately from surveillance conducted to protect national security—against foreign powers.[36] The Electronic Communications Privacy Act (ECPA) of 1986 covers the former; the Foreign Intelligence Surveillance Act (FISA) of 1978, the latter. Both have been amended significantly since their original enactment, most recently by the USA PATRIOT Act.[37] The ECPA consists of three separate acts: the Wiretap Act applies to the interception of the contents of communications like telephone calls and emails as the communication is occurring;[38] the Stored Communications Act applies to communications in electronic storage—for instance, an email on a server—as well as customer records held by telephone companies and internet service providers;[39] and the Pen Register Act applies to the installation of devices that capture information on outgoing calls (pen registers) and incoming calls (trap-and-trace devices), as well as the use of "processes" that capture similar information on internet users.[40] The type of surveillance contemplated by FISA parallels to some extent the ECPA's scheme: the interception of communications[41] and the installation of pen registers and trap-and-trace devices (as well as their internet equivalents).[42] FISA also sets down standards for a number of other types of information-gathering: video surveillance,[43] physical searches of premises,[44] and access to physical records like library borrower lists.[45]

Collecting call data, quite obviously, does not count as the interception of the contents of a communication, either in transmission or in storage.[46] Neither did the NSA install pen registers and trap-and-trace devices on individual phone lines to obtain the information. It used a far more efficient method: it piggy-backed off telecommunications providers, requesting that information already gathered in the course of routine business operations be transferred to the government. Hence the one piece of federal electronic surveillance law that does apply, squarely, to the kind of data involved

---

[36] For an overview of the electronic surveillance law discussed in this section, see SOLOVE, ROTENBERG & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note__at 267-97.
[37] The USA PATRIOT Act was passed in 2001 and reauthorized with amendments in 2006.
[38] 18 U.S.C. §§ 2510-2522.
[39] 18 U.S.C. §§ 2701-2711.
[40] 18 U.S.C. §§ 3121-3127.
[41] 50 U.S.C. §§ 1801-1811; *see generally* Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1322-29.
[42] 50 U.S.C §§ 1841-1846 (2000).
[43] 50 U.S.C. § 1804.
[44] 50 U.S.C. § 1821-29.
[45] 50 U.S.C. § 1861-62.
[46] The following discussion was informed by blog commentary by three experts on surveillance law. *See* Orin Kerr, More Thoughts on the Legality of the NSA Call Records Program (May 12, 2006), http://www.orinkerr.com; Peter Swire & Judd Legum, Telecos Could Be Liable For Tens of Billions of Dollars For Illegally Turning Over Phone Records (May 11, 2006), http://thinkprogress.org.

in the NSA program is that part of the Stored Communications Act on customer records.[47]

The Act bans companies from disclosing their customer records to the government,[48] but then creates a number of exceptions to that ban.[49] If the government obtains a warrant, a court order, or, for certain types of customer information, an administrative subpoena, then disclosure is permitted.[50] The warrant and court order procedures must be used for ordinary criminal investigations, the speedier administrative process may be used "in an authorized investigation to protect against international terrorism or clandestine intelligence activities."[51] These administrative subpoenas are known as National Security Letters.[52] If the Director of the FBI or his designee certifies that the customer records are being requested for an investigation "to protect against international terrorism or clandestine intelligence activities," the telecommunications provider must hand over the information.[53] Government access to customer data, therefore, replicates the more general, two-track approach to surveillance—one for law enforcement, the other for national security. Yet even though the call data was requested for national security purposes, administrative subpoenas were not used. At first blush, therefore, it appears that the NSA, along with the telecommunications providers that collaborated with the NSA, violated the Stored Communications Act.[54]

What would be the consequences of such a violation? As it turns out, they are fairly paltry as compared to those for other types of violations such as illegal wiretapping or illegal access to stored communications. There are no criminal penalties for breaching the customer-data provisions.[55] Against the telecommunications providers, individuals have a civil right of action for injunctive relief and damages, set at a statutory minimum

---

[47] Section 222 of the Communications Act also applies: it requires telecommunications carriers to keep their customer information confidential. 47 U.S.C. § 222. The duty of confidentiality, however, is subject to any disclosures required by law and therefore the analysis is similar to that under the Stored Communications Act.

[48] See Stored Communications Act, 18 U.S.C. § 2702(a)(3). The lawyers for the NSA might quibble that the NSA did not obtain information *on* a "subscriber to or customer of [an electronic communication] service," 18 U.S.C. §§ 2703(c)(1) & (2), since it only obtained data on phone numbers, without the names of the customers using those phone numbers. But the NSA request certainly comes within the spirit of the statute, given that the name of a subscriber can easily be identified based on her phone number and that the intent of the Act is to protect customer privacy.

[49] See 18 U.S.C. § 2702(c).

[50] See 18 U.S.C. § 2702(c)(1); 18 U.S.C. § 2703 (c)(1) & (2). The scheme for government access to financial records and credit reports is quite similar.

[51] 18 U.S.C. § 2709(b). This is the standard for *federal* administrative subpoenas. The statute, however, also contemplates administrative subpoenas issued by state entities and governed by state law. *See* 18 U.S.C. § 2703(c).

[52] SOLOVE, ROTENBERG & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note__at 728-29.

[53] 18 U.S.C. § 2709(b).

[54] The other circumstances under which a communications provider may lawfully disclose customer records are set out in 18 U.S.C § 2702(c)(2)-(6). From the information available in the media, it does not appear that the actions of the telecommunications providers would be covered by any of these provisions. As for the government, the statute contemplates two other means of obtaining the customer data, *see* 18 U.S.C. § 2703(c)(1)(C)&(D), neither of which are relevant here.

[55] 18 U.S.C. § 2701 (defining an offense as "access to a wire or electronic communication while it is in electronic storage").

of $1,000 per individual.[56] Against the government, they have a right of action for money damages, set at a minimum of $10,000 per person.[57]

Why, though, a violation only at first blush? Because the legal analysis must take into account the President's inherent constitutional power, under Article II, to authorize the call database. And, as with the constitutional case law, the different treatment of the content of communications and the incidents of communications—customer records—is critical: the legislative scheme is comprehensive with respect to the former, patchy on the latter. The President's authorization, therefore, might very well save the NSA program.

On this aspect of the legal analysis, it is useful to consider another NSA surveillance program—the warrantless wiretapping of telephone calls between individuals in the United States and individuals abroad. A group of legal scholars have mounted a forceful argument against this program.[58] They claim, for good reason, that the warrantless wiretapping program is illegal.[59] Their argument rests on Congress's comprehensive regulation of content-based surveillance in the ECPA and FISA—both of which require a warrant. The argument: Because these statutes, by their express terms, cover the entire universe of government wiretapping, the President has no other legal avenue for authorizing such wiretapping.[60] He cannot rely on Congress's later-in-time Authorization for the Use of Military Force because nothing in the broad, vague language of that statute suggests that Congress intended to override the explicit terms of the earlier surveillance statutes.[61] Neither can the President rely on his Article II powers.[62] According to Justice Jackson's classic tripartite scheme of presidential powers, the Present's authority to act turns, in large measure, on whether Congress has acted. In Justice Jackson's famous words

---

[56] 18 U.S.C. § 2707.

[57] 18 U.S.C. § 2712.

[58] *See January 9, 2006 Letter from Scholars and Former Government Officials to Congressional Leadership in Response to Justice Department Letter of December 22, 2005*, 85 IND. L.J. 1364 (2006); *February 2, 2006 Letter from Scholars and Former Government Officials to Congressional Leadership in Response to Justice Department White Paper of January 19, 2006*, 85 IND. L.J. 1415 (2006); July 14, 2006 Letter from Scholars and Former Government Officials to Congressional Leadership in Response to Justice Department Letter of July 10, 2006, available at http://www.law.duke.edu/publiclaw/pdf/lettertocongress7-14.pdf [hereinafter "Letter of July 14, 2006"].

[59] Indeed, the first federal court to decide the issue has held the program to be illegal. See ACLU v. National Security Agency/Central Security Service, Case No. 06-CV-10204, August 17, 2006 (E.D.Mich.).

[60] The pertinent section of the Wiretap Act says: "[p]rocedures in this chapter [Wiretap Act] or chapter 121 [Stored Communications Act] and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted." 18 U.S.C. § 2511(2)(f). The definition of both "electronic surveillance" and "interception of . . . communications" turns on access to the *content* of the communication.

[61] *See* Hamdan v. Rumsfeld, 126 S.Ct. 2749, 2775 (2006). In *Hamdan,* the Supreme Court held that the AUMF could not be construed as overriding the Uniform Code of Military Justice's requirements for military commissions.

[62] Letter of July 14, 2006, *supra* note__at 4.

> 1. When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate. . . .
>
> 2. When the President acts in absence of either a congressional grant or denial of authority, he can only rely upon his own independent powers, but there is a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain. . . .
>
> 3. When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter. Courts can sustain exclusive Presidential control in such a case only by disabling the Congress from acting upon the subject. Presidential claim to a power at once so conclusive and preclusive must be scrutinized with caution, for what is at stake is the equilibrium established by our constitutional system.[63]

Thus, in light of Congress's express instruction to the government to obtain a warrant—from an ordinary court in the case of criminal investigations and from the FISA court in the case of foreign intelligence—the President is at the "lowest ebb" of his powers in authorizing the warrantless surveillance program.[64] To save the program, he must show that Congress exceeded its constitutional powers, an uphill battle, indeed, in view of Congress's repeated and long-standing regulation of wire communications among states and between the United States and foreign nations under the Commerce Clause.[65] The President must also convince the Supreme Court that his national security and foreign relations powers extend to activities at the core of the Fourth Amendment—telephone conversations conducted by Americans in the privacy of their homes.

Returning to the NSA call-records program. With this program, the administration is on firmer ground because of the different statutory and constitutional treatment of call records. Although Congress has comprehensively regulated the various circumstances under which the government can listen to what is being said in telephone calls, it has not done the same for all the other information revealed by those calls. There is no equivalent provision on customer data that says the statutory procedures are to be "the exclusive means" of government access to such data. Neither is government access that flouts the statutory procedure criminalized. Thus the President's inherent constitutional power to authorize the call database is stronger than for warrantless wiretapping. He is acting in the less suspect "zone of twilight." Moreover, in authorizing the collection of call data, the President does not interfere with a constitutionally protected right to privacy. This difference is another reason why the call-records

---

[63] Youngstown Tube & Sheet Co. v. Sawyer, 343 U.S. 579, 635-38 (1952) (J. Jackson, concurring).
[64] *See* Letter of July 14, 2006, *supra* note__ at 4, 8.
[65] *See id.* at 6-7.

program might survive a legal challenge even if the warrantless wiretapping program does not.

This is not to say that, even under the less-demanding constitutional scrutiny of the "zone of twilight," the President would have the authority to order the transfer of call records from private telecommunications providers to the government. After all, the NSA database contains information on millions of telephone calls, the vast majority of which involved U.S. citizens and occurred entirely within the United States. This type of government initiative is a far cry from what has been traditionally understood as a power incident to the President's duty to protect the Nation from foreign threats. But it is worthwhile bringing attention to the consequences of the Supreme Court's and Congress's complacency in the face of government access to customer records, records that sometimes can be just as revealing to government investigators—and as private to citizens—as what is actually said in the telephone conversation.

Before concluding this discussion of U.S. law, one more piece of legislation should be mentioned. Once the calling records were transferred to the NSA they were put in a database and mined for terrorists. The first place to which a European would turn, faced with a similar European data-mining program, would be her data-protection law. In the United States, that would be the Privacy Act of 1974.[66] The Privacy Act regulates the federal government's collection, use, and disclosure of all types of personal information. It imposes a number of duties on government agencies: The responsible agency must alert the public to the existence of a personal records system by publishing a notice in the Federal Register. When information is collected from individuals, they must be told of the nature of the government database. The agency may gather only such information as is relevant and necessary to accomplishing the agency's legal purposes (purposes set down by statute or executive order). Personal information must be accurate, relevant, timely, and complete. This information cannot be transferred to another government agency without the consent of the person concerned. Technical measures must be adopted to guarantee the security and confidentiality of the information. Individuals have the right to check their personal information and, if necessary, demand that their information be corrected.

Compared to the law on government surveillance canvassed earlier, the reach of the Privacy Act is broader. It applies to the government's collection of all kinds of personal data, not just data related to one's telephone conversations (and a couple of other types of data protected under separate statutes such as bank account information). What is more, in contrast with the focus on government collection of information in surveillance law, the Privacy Act regulates the government's use of personal data from start to finish: collection, storage, use and analysis, transfers to other parties, and modification to accommodate changes over time.

---

[66] 5 U.S.C. § 552a. Useful discussions of the Privacy Act can be found in TRUDY HAYDEN & JACK NOVIK, YOUR RIGHTS TO PRIVACY 121-33(1980) and SOLOVE, ROTENBERG & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note__ at 579-83.

As we shall see, many of these guarantees parallel those of European privacy law. Yet the actual scope of individual rights under the Privacy Act is far more limited than under European laws: most of the government's duties are purely hortatory due to the limited enforcement mechanisms; a number of exceptions have been written into the Privacy Act; and the Act only applies to a narrow subset of what can be done, by the government, with personal information. Consequently, what would be a European privacy advocate's first line of defense against a government program involving such massive amounts of personal information turns out to be an entirely ineffective last resort in the United States.

Some more detail on the limitations of the Privacy Act: The only enforcement mechanism is a civil action in federal court, generally for damages.[67] Yet individuals have a very difficult time establishing the injury necessary to recover for most violations of the statute—what court would award damages because a government agency asked too many questions, and too many irrelevant questions? Moreover, the Privacy Act is riddled with exceptions. Disclosure of information to other agencies is permitted even without consent if the public is notified upfront, when the record system is created, that such disclosure constitutes a "routine use" of the information. This is defined as a use that is compatible with the main purpose for which the information was collected. Even without advance notice of a "routine use," personal information may be transferred to another agency if the transfer is for law enforcement purposes and is requested by the agency's head. Records held by law enforcement agencies and the CIA may be exempted from most of the requirements of the Act ("general exemptions") if the agency head publishes a notice to that effect.[68] Records held by any agency may be exempted from some of the requirements of the Act ("specific exemptions") if the agency head likewise publishes a notice to that effect and if they fall into one of a number of categories—investigatory material, statistical records, matters whose secrecy is in the interest of national defense or foreign policy, and more.[69] Finally, personal data held by the government is not considered a "system of records" covered by the Act unless the system is used by the agency to retrieve information about specific individuals, using the names, social security numbers, or other identifying particulars of those individuals.[70]

The call-records program is a perfect illustration of the limitations of the Privacy Act. Unlike the FBI and the CIA, the NSA does not qualify for a general exemption. In theory, therefore, the agency must comply with the bulk of the Privacy Act's requirements.[71] But Federal Register notices of NSA records systems generally take advantage of the specific exemptions for national security records. Plus, even without specific mention in the Federal Register, the NSA may share personal information with other government agencies if requested to do so for law enforcement purposes.[72] Perhaps the most troubling aspect of this analysis is the question of whether the call database

---

[67] *See* SOLOVE, ROTENBERG & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note__ 586.
[68] 5 U.S.C. § 552a(j).
[69] 5 U.S.C. § 552a(k).
[70] *See, e.g.*, Williams v. Dept. Veterans Affairs, 104 F.3d 670 (4th Cir. 1997).
[71] *See* National Security Agency/Central Security Service Privacy Act Program, 32 C.F.R. pt. 322 (2006).
[72] 5 U.S.C. § 552a(b)(7).

would even count as a "system of records" under the Privacy Act.[73] Is a phone number, without a name attached, an "identifying particular" assigned to an individual? If so, then it seems that searching the system by the phone number of an al Qaeda suspect, to obtain information on her activities or to identify other possible suspects would count as retrieving information about her. But what about using the country code for Afghanistan as a search term? Or, as is most likely the case, combining these and other criteria as part of complex algorithms to discover new relationships among the data and to generate presumably a better, more accurate pool of terrorists and terrorist activity. The few courts deciding the question of what is a "system of records" have reached different, inconsistent conclusions. And most of them have defined the term quite narrowly.[74] Absurdly, therefore, a database containing personal details on millions of citizens might fall entirely outside Congress's data-privacy scheme.[75] And again, following the logic of Justice Jackson's concurrence in *Youngstown*, the President would have a respectable argument that the database came within his inherent constitutional authority to protect national security.

IV. EUROPE: LEGAL IMPOSSIBILITY

In Europe, a secret government data-mining program like the NSA's would be clearly illegal. Why? To summarize the rather complicated analysis that follows, such a data-mining program would violate two different types of privacy guarantees—procedural and substantive. Procedurally, government data-mining, even for national security ends, would have to be authorized by a public law or regulation that specified the purposes of the personal data processing and the limits on that data processing, to minimize the government's interference with private life. Before the program could be enacted, an independent government body would have to be consulted and, while the program was in operation, that same government body would have to have oversight and enforcement powers. These procedural requirements improve the prospect that the privacy ramifications of new government initiatives will be fully debated and widely understood at the outset. During the life of the government program, these procedures improve the chances that privacy violations will be detected and remedied.

On the substance, the reach of a European data-mining program would be narrower than that of the NSA call database. Although a spy agency might be allowed access to all call information held by national telecommunications providers, it would not be allowed to retain the personal data as long as the NSA has—over five years now. Furthermore, the type of analysis performed on the data, as well as the uses of the results of the analysis would have to be carefully circumscribed. The government would be

---

[73] For instance, a report issued by the Congressional Research Service assumes that the Privacy Act does *not* apply to data-mining and suggests that Congress consider "the possible application of the Privacy Act to these [data-mining] initiatives." *See* Seifert, Data-mining and Homeland Security, *supra* note__at 19.
[74] *See, e.g.*, Jacobs v. National Drug Intelligence Center, 423 F.3d 512 (5th Cir. 2005); Williams v. Dept. Veterans Affairs, 104 F.3d 670 (4th Cir. 1997); Henke v. Dept. Commerce, 83 F.3d 1453 (D.C. Cir. 1996).
[75] In practice, given the far-reaching exemptions that apply even if the personal data is considered part of a system of personal records, this simply means that the NSA is not obliged to published a notice in the Federal Register.

permitted to use only search terms, statistical models, mathematical algorithms, and other analytical processes designed to uncover serious threats. Under German law, for instance, an international terrorist attack counts as serious, counterfeiting abroad does not.[76] And under German law, before the government may engage in data-mining there must be an "imminent and specific endangerment" (*konkrete Gefahr)* of a serious offense, not simply an "abstract endangerment" of international terrorism such as that existing in the aftermath of the September 11 terrorist attacks.[77] A spy agency in Germany would be allowed to pass on the names of individuals obtained through such data-mining techniques only if those individuals were suspected of planning to commit, or having already committed, a serious offense and only if sufficient reasons existed for entertaining that suspicion.[78]

Another substantive difference would be the right, under European law, of individuals to check on their information. This right of access enables individuals to ensure that their information is factually correct and that it is being handled in accordance with the guarantees of privacy law. Finally, to switch the focus briefly from the government to the private sector, the same amount of call data in the hands of telecommunications providers would not have been available to a European government. Under European law, telecommunications companies are prohibited from retaining personal data in the same quantities and for the same length of time as is routine—and legal—in the American business world.

Although, as we shall see, some of the substantive guarantees of European law are quite technical, at their root are values easily recognizable to the members of any liberal democracy. The most fundamental is what the legal philosopher Stanley Benn calls "respect for persons."[79] At the core of liberalism is the free, rational, equal person. The social contract rests upon this vision of individual autonomy—at one and the same time a product and promoter of this choosing being. From the perspective of the observer, acknowledging the privacy of another is respect for the choice made by that person to keep something for herself or her close circle of confidants. From the perspective of the observed, the right to keep certain matters private and make others public is critical to developing her identity as an autonomous person who freely chooses her own life projects. When the observer is the state, the failure to respect the choice for privacy has special consequences for liberty because of the substantial means at the disposal of the state. The total surveillance of George Orwell's 1984 could only be achieved by the state. Collecting, combining, and manipulating information on people is the digital equivalent of gazing at them without their consent. This liberty interest underpins the law of information privacy.

---

[76] *See* Bundesverfassungsgericht [BverfG] [Federal Constitutional Court] July 14, 1999, 1 Entscheidungen des Bundesverfassungsgerichts [BverfGE] 2226/94, 2420/95, 2437/95 (76) (F.R.G) [hereinafter "Judgment on G10 Amendments"] .

[77] *See* Bundesverfassungsgericht [BverfG] [Federal Constitutional Court] April 4, 2006, 1 Entscheidungen des Bundesverfassungsgerichts [BverfGE] 518/02 (F.R.G) [hereinafter "Judgment on Data-mining"].

[78] Judgment on G10 Amendments, *supra* note__at 85-87.

[79] Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, *in* NOMOS XII: PRIVACY 1 (J. Roland Pennock & John W. Chapman eds. 1971).

A second reason for shielding individuals from the gaze of others—and from the unfettered collection, storage, analysis, and retrieval of data about them—is to prevent all the illegitimate uses that can be made of knowledge about them. Suppression of speech and political protest, in the United States, is one of the most repugnant of these illegitimate uses. The attempt to draft Norwegian men into the German army based on what had been collected originally as innocent census data is another example. Discrimination based on religion, race, or ethnic origin is yet another harmful use of knowledge of others. Again, both other individuals and the government can commit these wrongs but, when the government is involved, the dangers are greater because of the tremendous resources at its command. Anti-terrorism data-mining, which makes heavy use of terrorist profiles based on sex (male), age (18–40 years), religion (Muslim), and country of origin (country with significant Muslim population), quite obviously triggers these discrimination and speech concerns.

The last set of reasons for information privacy is somewhat remoter from what is traditionally considered the core of privacy. One of these is the theft of personal data for fraudulent or other criminal purposes, a much greater risk with electronic data because of ease with which such data can be collected and copied. In the case of anti-terrorism data-mining, however, the foremost of these reasons is the danger of inaccuracy. Because of the ease with which electronic data can be gathered, stored, and combined in the age of information technology, the accuracy of that data is difficult to guarantee. This is not simply because it is often wrongly recorded, through human error. When different data sets are combined, their different coding and software systems can lead the information in one of the data sets to be wrongly interpreted, based on the other data set's coding and software system. What is more, electronic data is so easy to store that it can remain long after the facts on the ground have changed and, therefore, it has become inaccurate. A valid data-mining process, as describe earlier, is dedicated in large part to fixing these inaccuracies. The questionable quality of electronic data is cause for concern because of the great reliance placed on such data by all types of actors in making a vast number of decisions with adverse consequences for the individuals concerned. When data is being mined to detect terrorists, these consequences are especially grievous: being wrongly surveilled, detained, prosecuted, even convicted.

Before going any further, it is necessary to clarify what is meant by "Europe." Personal data processing for purposes of national security and law enforcement is covered by two Europe-wide instruments—the European Convention on Human Rights (ECHR) and the Council of Europe Convention on Personal Data Processing.[80] It is also covered by individual national laws. This article will focus on the laws of Germany and France because of their longstanding influence at the European level and, through instruments at the European level, on other national legal systems. The law of another Europe-wide organization—the European Union—has not historically had much of a role in this area because of the limitations on the organization's powers. The European Union, until recently, has been responsible for creating a common market, not for

[80] Council of Europe Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. No. 108 [hereinafter "Convention," "Convention 108" or "Council of Europe Convention"].

policing or protecting national security. That constitutional structure is gradually changing, in the face of the expanding powers of the European Union, but the basic point is still valid. This discussion, therefore, will only raise EU law selectively, for the few issues on which it is germane.

In European law, the main line of defense against data-mining is general data-protection law, not sectoral legislation as in the United States. The call records in this hypothetical are considered a subset of personal data—albeit a more protected subset of personal data than, say, one's home address. For the very same set of facts, the source of government duties and individual rights is the law of telecommunications surveillance in the United States, the general law of data privacy in Europe. Of course, there is telecommunications law in Europe. At the constitutional level, however, only in Germany is the privacy of communications and data related to communications afforded protection under a separate article of the Constitution and a separate line of cases.[81] And even there, the constitutional reasoning is, for all intents and purposes, identical to the reasoning in the data-privacy cases. At the statutory level, the law regulating telecommunications surveillance—which in Europe squarely includes the collection of non-content data—always requires an individualized suspicion of wrong-doing before the communications data may be intercepted by, or transferred to, the government.[82] The one

---

[81] Grundgesetz für die Bundesrepublik Deutschland [GG][Basic Law], art. 10. Article 10 says: "The confidentiality of letters, as well as the confidentiality of post and telecommunications is inviolable." SABINE MICHALOWSKI & LORNA WOODS, GERMAN CONSTITUTIONAL LAW: THE PROTECTION OF CIVIL LIBERTIES 293 (1999). In 1999, the Constitutional Court explained that Article 10 includes both the content of communications and non-content data (called "connection data"):

> The protection of fundamental rights, however, is not restricted to shielding the content of an act of communication against the state taking note of it. The protection of fundamental rights also covers the circumstances of communication, particularly including: (1) information about whether, when and how often telecommunications traffic has taken place or has been attempted; (2) information about the individuals between whom telecommunications traffic has taken place or has been attempted; and (3) information about which subscriber lines have been used. The state cannot, in principle, claim to be allowed to take note of the circumstances of acts of communication. The use of the medium of communication is supposed to remain confidential in all respects.

Judgment on G10 Amendments, *supra* note__at 51-52 (citations omitted).

[82] In France, electronic surveillance, including the monitoring and collection of non-content data ("*données techniques*"), is regulated differently depending on whether it is conducted as part of a criminal investigation or for intelligence purposes. In the law enforcement context, such surveillance is known as "judicial surveillance" (*écoutes judiciares*) because the authorizing order is issued by a member of the judicial branch. *See* CODE DE PROCÉDURE PÉNALE [C. PR. PÉN.] arts. 100-100-7 (interception of communications), arts. 60-1, 77-1, 99-3 (police access to telecommunications data). In the intelligence context, electronic surveillance is known as "administrative surveillance" (*écoutes administratives*) because the order is issued by a member of the government, generally the Minister of the Interior, and is reviewed by an independent agency (the Commission nationale de contrôle des interceptions de sécurité or CNCIS). *See* Law No. 91-646 of July 10, 1991, art. 3 (interception of communications); Law No. 2006-64 of January 23, 2006, art. 5 (access to telecommunications data). In Germany, the same distinction exists, albeit complicated by the federal organization of the German state. All telecommunications surveillance conducted for purposes of bringing a criminal prosecution is governed by Section 100a of the Code of Criminal Procedure (Stafprozessordnung or StPO). Surveillance conducted by the Länder police for purposes of preventing ordinary crime is governed by the police laws of the Länder. Domestic security surveillance—conducted by the federal Office for the Protection of the Constitution (Bundesamt fur Verfassungschutz or BfV) and the BfV's counterparts at the Land level—is regulated by a separate federal

exception to this requirement is the German legislation on foreign intelligence surveillance, which contemplates not only individualized surveillance but also "strategic surveillance."[83] Strategic surveillance is similar to data-mining in that large numbers of telephone calls and other forms of communications are intercepted, without a particularized suspicion of wrongdoing, and then screened using certain search terms. Strategic surveillance is only permitted, however, for communications *with foreign nations* and only to prevent international terrorist attacks and other types of national security threats. Purely domestic phone calls are excluded. In sum, the general provisions of telecommunications law could not be used to authorize the massive transfer of customer data to the government for data-mining purposes. Rather, in Europe, a government initiative like the NSA's would require a new law or regulation and that law or regulation would have to satisfy both fundamental rights standards on data privacy as well as the requirements of general data-protection legislation.

Turning to those standards. The privacy of personal information is considered a fundamental right at both the European and national levels: the right to respect for private and family life in the European Convention on Human Rights,[84] the right to informational self-determination[85] and the privacy of communications[86] in Germany, and

---

law, the G10 Law. Foreign security surveillance, mostly the responsibility of the Federal Intelligence Service (Bundesnachrichtendienst or BND), is covered by the same federal law. *See generally* Jacqueline Ross, *Germany's Federal Constitutional Court and the Regulation of GPS Surveillance*, 6 GERMAN L.J. 1805, 1812 (2005) (explaining organization and statutory regulation of German intelligence and law enforcement agencies). In the wake of September 11, the BfV and the BND obtained broader access to customer data held by telecommunications providers and financial institutions. BGBl. I 2002 at 361. Still, however, requests for communications and financial data must be particularized: the BfV must suspect an individual of engaging in activities aimed at overthrowing the constitutional order; the BND must suspect an individual of being an actual (*tatsächlich*) danger to the foreign and security policy interests of Germany.

[83] This is the G10 Law of 1968, so-called because the law amended Article 10 of the Basic Law and gave effect to the second paragraph of that Article. *See* BLANCA R. RUIZ, PRIVACY IN TELECOMMUNICATIONS: A EUROPEAN AND AN AMERICAN APPROACH 218, 267 (1997); Paul M. Schwartz, *German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance*, 54 HASTINGS L.J. 776, 778-779 (2002-2003).

[84] European Convention of Human Rights art. 8. *See* Malone v. The United Kingdom, Application No. 8691/79, para. 84 (Aug. 2, 1984) (holding that pen registers constitute an interference with private life under Article 8); Leander v. Sweden, Application No. 9248/81, para. 48 (Mar. 26, 1987) (holding that recording of personal details in police files constitutes interference with private life under Article 8); Rotaru v. Romania, Application No. 28341/95 (May 4, 2000) (holding that storage and use of personal information in police file, together with refusal of right of correction, amounts to interference with private life under Article 8); *see also* Opinion of Advocate General Léger, Joined Cases C-317/04 and C-318/04, European Parliament v. Council, paras. 207-32 (Nov. 22, 2005) (finding that all personal data gathered by the police is covered by Article 8); Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, 2005 O.J. (C 298) 1, para. 9 (same).

[85] This constitutional right is based on the right to human dignity (Article 1) and the right to free development of one's personality (Article 2.1). *See* DONALD P. KOMMERS, THE CONSTITUTIONAL JURISPRUDENCE OF THE FEDERAL REPUBLIC OF GERMANY 323, 324-25 (2d ed. 1997) (Census Act Case).

[86] Grundgesetz für die Bundesrepublik Deutschland [GG][Basic Law], art. 10.

the right to respect for private life in France.[87] All information that is about a specific person is considered personal and therefore deserving of privacy. If the government wishes to interfere with this right, it must do so based on a law that is accessible to the public and that contains provisions precise enough to curb arbitrary government action and to put citizens on notice of possible incursions into their private sphere.[88] The purpose of the interference with privacy must be legitimate. Protecting "national security," guaranteeing "public safety," and preventing "disorder or crime" are specifically listed as legitimate purposes under Article 8 of the ECHR. The European Court of Human Rights has consistently ruled in favor of government legislation with such aims.[89] Likewise, the German and French constitutional courts have repeatedly found preventing crime, fighting terrorism, and protecting national security to be legitimate public reasons for impinging upon individual rights.[90]

Fundamental rights law requires that the government's—legitimate—interference with privacy be proportional. The proportionality test pervades the case law of all the European courts under consideration, on all rights, not simply the right to privacy.[91] Proportionality generally turns on three related inquiries: Can the government action can achieve the stated purpose? Is the government action necessary for accomplishing the stated purpose or are there alternative means of accomplishing the same purpose that will burden the right less? And, when a non-economic right is at stake, even though there might be no alternative means for accomplishing the same purpose, is the burden on the right nonetheless intolerable, requiring the law to be withdrawn? Of course, this formulation greatly simplifies the doctrine of proportionality. The test differs not only among courts, but as between different cases decided by the same court. Moreover, the burden of justification on the government varies tremendously depending on the right at stake and the public interest being pursued: the more important the right, the higher the

---

[87] *See* CC decision no. 94-352, Jan. 18, 1995 (Loi d'orientation et de programmation relative à la sécurité); CC decision no. 2004-499 DC, July 29, 2004, recital 2 (Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel). The respect for private life is recognized by the Constitutional Council as one of the liberties protected under Article 2 of the Declaration of the Rights of Men and Citizens of 1789, which is considered part of the French Constitution of 1958 by virtue of the reference to the Declaration in the preamble to the Constitution.

[88] This is the interpretation given by the European Court of Human Rights to the requirement, under Article 8, that "[t]here shall be no interference by a public authority with the exercise of his right [to private life] except such as is in accordance with the law . . . ." *See, e.g.*, Peck v. The United Kingdom, Application No. 44647/98, para. 76 (Jan. 28, 2003). Under German constitutional law, laws that authorize government interference with certain basic rights must be *parliamentary* laws. In other words, they must be laws directly voted on by the representatives of the people; they cannot be regulations promulgated by the executive branch, based on authority delegated by the parliament. This is the case for government restrictions on the right to the confidentiality of telecommunication and the right to informational self-determination. *See* RUIZ, PRIVACY IN TELECOMMUNICATIONS, *supra* note__ at 194-96.

[89] *See, e.g.*, Klass and Others v. Germany, Application No. 5029/71 (Sept. 6, 1978); Khan v. The United Kingdom, Application No. 35394/97 (May 12, 2000).

[90] *See* Schwartz, *German and U.S. Telecommunications Privacy Law*, *supra* note_ at 771-82 (German Constitutional Court); CC decision no. 2005-532DC, Jan. 19, 2006 (French Constitutional Council).

[91] *See* Gilles Dutertre, KEY CASE-LAW EXTRACTS: EUROPEAN COURT OF HUMAN RIGHTS 240, 307, 311, 347, 368 (2003) (European Convention on Human Rights, arts. 7, 8, 9, 10, 11, 14); KOMMERS, THE CONSTITUTIONAL JURISPRUDENCE OF THE FEDERAL REPUBLIC OF GERMANY, *supra* note__ at 46 (Germany); CC decision no. 94-4352 DC, Jan. 18, 1992, 2nd recital (France).

burden on the government; the more important the public purpose, the lower the burden on the government. Nonetheless, it is useful to establish a least-common-denominator point of reference.

When the privacy right is data privacy and when the government interference is for purposes of law enforcement or national security, more specific conditions must also be met: the terms of the Council of Europe Convention and national data-protection laws. Whereas the former sets down general data-protection commitments, the latter give effect to, and elaborate extensively upon, those commitments. In 1981, the members of the Council of Europe concluded the Convention on Personal Data Processing.[92] The Convention is critical to understanding European data protection. Of all the Europe-wide instruments on data protection, it has the broadest coverage, both regarding subject-matter and geographically. The Convention, unlike EU data-protection laws, applies to all types of personal data processing, by both government and private actors. It has been ratified by thirty-eight of the forty-six members of the Council of Europe and it has been signed, but not yet ratified, by four more member states. That is a considerably broader group of nations than the membership of the European Union.[93] Furthermore, because of the Convention's age, it has been influential in developing data-protection legislation everywhere in Europe. National latecomers to the policy area like the United Kingdom copied, whole cloth, the terms of the Convention into their domestic data-protection legislation at the time of implementation. The European Union has used the Convention's general principles as the framework for the more detailed provisions of its data-protection law governing market actors.[94] Other EU data-protection rules copy directly from the Convention.[95]

The data-protection laws of Germany and France also have particular significance. National data-protection legislation is generally categorized according to historical vintage: the first generation, enacted in the 1970s; the second generation, dating to the 1980s and adopted to implement the Convention; and the third generation, adopted in the late 1990s and early 2000s to fulfill the requirements of membership in the European Union.[96] The German and French laws belong, squarely, to the first generation. Because of their early vintage, they were influential blueprints for the Council of Europe Convention. And as a result of Germany's and France's extensive regulatory experience, their legal instruments—and their data-protection officials—continue to exercise influence, both on novel questions of data protection and on countries in the process of adopting their first data-protection legislation.

---

[92] *See* COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY 71-74 (2003).
[93] This wider geographic scope is true even taking into account the non-EU members who have adopted EU data-protection instruments pursuant to association agreements with the European Union.
[94] Council and Eur. Parl. Directive 95/46/EC 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.
[95] Schengen Acquis—Convention Implementing the Schengen Agreement of 14 June 1985 Between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the Gradual Abolition of Checks at Their Common Borders, 2000 O.J. (L 239) 19, art. 115; Convention Based on Article K.3 of the Treaty on European Union, on the Establishment of a European Police Office (Europol Convention), 1995 O.J. (C 312) 2, art. 14.
[96] *See* BENNETT & RAAB, THE GOVERNANCE OF PRIVACY, *supra* note__at 102-03.

In Germany, the Federal Data Protection Act was originally enacted in 1977, and significantly amended in 1990 and 2001. It covers private actors throughout Germany,[97] including telecommunications companies and federal public bodies, including Germany's federal law enforcement and intelligence agencies.[98] An independent agency, known as the Federal Data Protection Commissioner, has been established to enforce federal data-protection law.[99] In addition, a special oversight system has been established for telecommunications surveillance—including surveillance of non-content data—conducted by domestic and foreign intelligence agencies: a parliamentary commission, known as the G10 Commission, reviews all individual surveillance orders as well as the administrative rules governing data-mining procedures used in strategic surveillance.[100] Each Land also has a Data Protection Act.[101] These acts set down the data-protection rules that discipline state government; they create Land data-protection authorities, to enforce the Land rules as well as the Federal Data Protection Act's provisions on market actors. (In Germany's federal system, state government is entrusted with implementing and enforcing most federal legislation.[102]) Land data-protection rules are also pertinent to intelligence-gathering for purposes of preventing terrorism: the Lander all have their own police forces, responsible not only for criminal investigations but also for protecting public order against future offenses ("preventive policing") and governed by Land laws.[103]

In contrast with federal Germany, France is a unitary system. This greatly simplifies the legislative scheme—it has only one data-protection law and one data-protection law enforcer. The Law on Data Processing, Data Files and Individual Liberties (Law No. 78-17) was enacted in 1978 and significantly amended in 2004.[104] It regulates data processing throughout the economy and throughout government, including the police and national security agencies. An independent agency (the Commission Nationale de l'Information et des Libertés or "CNIL") is entrusted with extensive enforcement powers: it is charged with registering and authorizing certain types of data-processing operations, with promulgating interpretive regulations, with conducting inspections and imposing administrative sanctions, and with advising the government on legislative and regulatory measures affecting privacy.

---

[97] Bundesdatenschutzgesetz [Federal Data Protection Act], May 22, 2001, BGBl.I at 904, § 27 (F.R.G.) [hereinafter "Federal Data Protection Act"].
[98] *Id.* § 12.
[99] COLIN J. BENNETT, REGULATING PRIVACY 77-90 (1992); DAVID FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 22-24 (1989).
[100] *See* RUIZ, PRIVACY IN TELECOMMUNICATIONS, *supra* note__at 218-20; 272-74; Judgment on G10 Amendments, *supra* note__at 92-93.
[101] *See* FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES, *supra* note__at 25.
[102] *See* DAVID P. CURRIE, THE CONSTITUTION OF THE FEDERAL REPUBLIC OF GERMANY 69-76 (1994).
[103] *See* Ross, The Elusive Line Between Prevention and Detection of Crime in German Undercover Investigations, *supra* note__ at 7, 25, 28. However, the surveillance activities of the Land agencies charged with national security (Landesamt für Verfassungsschutz) are governed exclusively by federal law, namely the G10 Law.
[104] Law no. 78-17 of Jan. 6, 1978, as amended by Law no. 2004-801 of Aug. 6, 2004, Journal Officiel de la République Française [J.O] [Official Gazette of France], Aug. 7, 2004 (hereinafter "Law no. 78-17"]; s*ee* FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES, *supra* note__at 80.

Fundamental rights law is the basic frame for the Council of Europe Convention and the German and French legislation. They contain a specific set of conditions designed to satisfy the requirements of legitimacy and proportionality in those instances in which the right to *data* privacy is burdened.[105] Paralleling the fundamental rights doctrine on the need for an authorizing law, personal data should be processed fairly and lawfully.[106] Since a fundamental right is at stake any time an individual's personal data is processed, such data must be stored for specified and legitimate purposes and should only be used in accordance with those purposes.[107] The *amount* of the data processed should be no more than necessary to accomplish the purpose.[108] Neither should the *time* during which the data are stored be any longer than necessary to accomplish the purpose.[109] The data must be accurate and, whenever necessary, kept up to date—otherwise, how would such data processing be able to achieve the stated purpose?[110] Types of personal data that are believed to be especially sensitive, for instance, data revealing racial origin, religious beliefs, and health conditions must be afforded "appropriate safeguards."[111] Those who process personal data must put into place "appropriate security measures" to ensure that personal information will be revealed only to those for whom it is intended.[112] As a special safeguard for the burdened privacy right, individuals should have the right to check their personal data, to make sure that it is accurate and that, in all other respects too, their personal data is being processed in accordance with the law.[113] All these guarantees can be found in the German and French data-protection laws, albeit in more detailed incarnations.[114]

The state parties are allowed to derogate from the Convention's provisions in the interests of "protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences."[115] These are interests clearly at stake in our hypothetical. Such derogations, however, must be detailed in the state party's national law and must be necessary, meaning that they must be carefully justified like any other government interference with the right to privacy. Both the German and the French legislation take advantage of this possibility; exceptions exist for data processing for intelligence and law enforcement purposes.[116] In neither case, however, is such data

---

[105] *See, e.g.*, Rotaru v. Romania, *supra* note__, at para. 3 (relying on Convention 108 in interpreting European Convention on Human Rights, art. 8).
[106] Convention 108, art. 5a. Even more precise is the German Federal Data Protection Act, *supra* note __ § 4. It says: "The collection, processing and use of personal data shall be admissible only if permitted or prescribed by this Act or any other legal provision or if the data subject has consented."
[107] Convention 108, art. 5b.
[108] *Id.* art. 5c.
[109] *Id.* art. 5e.
[110] *Id.* art. 5d.
[111] *Id.* art. 6.
[112] *Id.* art. 7.
[113] *Id.* art. 8.
[114] *See, e.g.*, Federal Data Protection Act §§ 19-21, 33-35 (rights of the data subject); Law 78-17, arts. 38-43 (rights of individuals in respect of processing of personal data).
[115] Convention 108, art. 9.2a.
[116] *See, e.g.*, Federal Data Protection Act §§19(3), 19(4); Law 78-17, art. 41.

processing, by the relevant government agencies, entirely or even mostly exempt from the safeguards of national data-protection law.

Another distinguishing feature of European data-privacy law is the enforcement system. Independent agencies responsible for the enforcement of data-protection law have been established in all European countries.[117] To these national agencies, add the supranational bodies responsible for overseeing compliance in the European Union: the European Data Protection Supervisor, with jurisdiction over EU institutions responsible for common market regulation;[118] the Joint Supervisory Body with jurisdiction over personal data exchanged through Europol;[119] and the Joint Supervisory Authority with jurisdiction over personal data exchanged through Schengen.[120] The powers of these national and supranational privacy agencies vary, but most, including the German and French data-protection authorities, have the power to review proposed laws and regulations with a data-protection impact, to conduct inspections of private and public data processors, and to commence administrative proceedings against violators, which may result in injunctive orders or administrative fines.[121] Since many violations of national laws are considered criminal offenses, such agencies also have the power to

---

[117] *See* BENNETT & RAAB, THE GOVERNANCE OF PRIVACY, *supra* note__ at 106, 108.

[118] *See* Regulation No. 45/2001 of the Eur. Parl. and of the Council, 2001 O.J. (L 8) 1 (on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data).

[119] *See* Convention Based on Article K.3 of the Treaty on European Union on the Establishment of a European Police Office (Europol Convention), *supra* note__art. 24. Europol is located in The Hague, Netherlands. It was established by the Member States to support their police forces and other national law enforcement authorities such as customs agencies, immigration services, and border and financial police. Europol's remit covers serious organized crime with an international dimension, including terrorism. It is to assist national authorities in combating international organized crime by collecting, analyzing, and transmitting intelligence to those authorities. Its information comes from national law enforcement bodies, as well as international agencies. Europol, however, does not have any enforcement or police powers; Europol information is used for *national* police investigations.

[120] The Schengen acquis—Convention Implementing the Schengen Agreement of 14 June 1985 Between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the Gradual Abolition of Checks at Their Common Borders, *supra* note __ art. 115. Schengen was originally created by a small group of Member States to jointly manage the admission of foreign citizens to their territories. The key elements of the scheme are a common visa—recognized by all state parties—and the removal of internal border controls among the state parties. Currently, the signatories are the EU Member States, with the exception of Ireland and the UK, and three EFTA countries—Iceland, Norway, and Switzerland. Fifteen of the 26 signatories have implemented the Schengen agreement. To enable national authorities to monitor foreign citizens admitted on the common visa, a secure database known as the Schengen Information System (SIS) has been established. Unlike the Europol system, the information contained in the SIS is not collected and analyzed centrally. Rather, national police and law enforcement authorities independently enter and extract information from the system. The data contained in the SIS is extremely varied: loss or theft of passports and other identity documents, names of individuals suspected of having committed serious crime, extradition warrants, car thefts, and more. As should be clear from this list of data, the SIS is no longer used solely for enforcing immigration policy. It has become a general purpose database for fighting crime with a cross-border element.

[121] *See* Federal Data Protection Act §§ 22-26 (setting down composition and powers of Federal Commission for Data Protection), § 38 (setting down requirements for Land data-protection authorities), §§ 43-44 (setting down administrative and penal sanctions for breaches of Federal Data Protection Act); Law 78-17, arts. 11-21 (establishing composition and powers of CNIL), arts. 45-49 (setting down administrative sanctions), arts. 50-52 (setting down criminal sanctions).

bring prosecutions directly or to refer privacy violations to public prosecutors for further action.

A final important aspect of European privacy law is the application of the law to public and private actors alike. At the level of fundamental rights, the guarantees of the ECHR and the German Basic Law have been applied to privacy violations committed by private actors, not only the government.[122] At what might be termed in the European hierarchy of legal norms, the statutory level, data-protection guarantees are binding on both public and private users of personal data. Thus, in the Council of Europe Convention, no distinction is made between the duties of private and public actors. Given the greater specificity of legislation at the national level, the French and German laws do separate public from private data processing, but only for purposes of stipulating special duties that apply to certain types of data processing such as that involving national identification numbers.

Now to apply European law to the facts of our hypothetical. Would a secret presidential directive count as a "law" for purposes of the fundamental rights analysis? No. By definition, a secret directive is not accessible to the public. It cannot put citizens on notice of how their government is interfering with their basic rights. Nor can it curb potential abuses of government power, since no one but those government officials know the limits placed on their power by the directive.

European law, of course, permits exceptions to data privacy based on national security concerns, though surely not on the scale suggested by the U.S. President, who has claimed that *any* disclosure of the NSA call database threatens national security.[123] One useful indicator of how such a claim would be addressed in Europe is a German constitutional case involving the G10 Law. That law, enacted in 1968, provides for wide-ranging surveillance by Germany's domestic and foreign security agencies to "ward off dangers which threaten the free democratic order, the existence or the safety of the Federal Republic of Germany or of one of the German Länder." Two types of surveillance are contemplated: individual monitoring and strategic surveillance. Strategic surveillance closely resembles the NSA's data-mining: the Federal Intelligence Service automatically screens phone traffic between Germany and certain foreign nations based on certain search terms and refers the resulting calls to government agents for further scrutiny.

---

[122] *See* Von Hannover v. Germany, Application No. 59320/00 (June 24, 2004) (applying Article 8 in case of privacy violation by the media); RUIZ, PRIVACY IN TELECOMMUNICATIONS, *supra* note__ 302-13 (discussing German constitutional doctrine of "horizontal" effect of rights (*Drittwirkung*) and the application of the doctrine in the case of Art. 10 of the Basic Law); Amtsgericht Berlin-Mitte [Berlin Center District Court], Geschäftsnumber [Docket No.] 16 C 427/02 (Dec. 18, 2003) (F.R.G) (holding for plaintiff in suit by pedestrian against Berlin department store for removal of surveillance cameras based on Basic Law, Arts. 1&2 and Federal Data Protection Act).

[123] *See generally* Memorandum from Congressional Research Service on Statutory Procedures Under Which Congress Is To Be Informed of U.S. Intelligence Activities, Including Covert Actions, Jan. 18, 2006, p. 9.

When the G10 Law was amended in 1994 to expand the list of threats warranting surveillance, a constitutional challenge was brought against the provisions on strategic surveillance. The challenge involved the government's duty to inform individuals who were targeted for further surveillance as a result of these random searches of international phone traffic, together with the oversight powers of the responsible parliamentary commission. The Court found that individuals had the right to be notified, but that notification could be delayed until such time as revealing the surveillance would no longer undermine national security or other important government interests.[124] The Court also held that the government had a duty to inform the parliamentary oversight commission both of the ministerial orders specifying the countries and search terms used in the surveillance and of the further steps taken, once a particular communication had been identified as suspicious and targeted surveillance had been triggered.[125] Given this reasoning, it is highly unlikely that the German Constitutional Court would approve of keeping an entire surveillance program secret. Any slight advantage that the government might gain from keeping secret a database involving the personal data of millions of citizens not individually suspected of terrorism would almost certainly be outweighed by the harm to the fundamental right to privacy.

The good news for the call database is that it would satisfy the second requirement of European fundamental rights law: collecting call data and mining it to protect against terrorist attacks is, most certainly, a legitimate purpose.

But what about proportionality? Can a database with the calling records of tens of millions of citizens be necessary to fight terrorism? European courts and privacy officers show considerable deference to their intelligence services in making this kind of determination. They are acutely aware of their limits in understanding how to combat terrorism, as compared to the seasoned professionals in their national spy agencies. But, in Europe, an argument would have to be made that data collection was capable of reducing the terrorist threat.

One good illustration of the case that would be expected from a European government is the debate leading up to the EU Data Retention Directive of March 2006.[126] Under the Directive, providers of electronic communications services and networks are required to keep traffic data related to phone calls, emails, and other communications for a period of six months to two years, depending on the Member State. Such data must be made available to the national police and, via national police, to police officers in other Member States. The purpose of the Directive is to fight serious crime, most notably terrorism. Notwithstanding this purpose, the Directive applies to market actors; it was therefore adopted as a common market measure. In proposing the Directive, the national governments in the Council of Ministers put forward a study based on the experience of the British police showing that call data older than six months was

---

[124] Judgment on G10 Amendments, *supra* note__at 89.
[125] *Id.* at 92.
[126] Directive 2006/24/EC, 2006 O.J. (L 105) 54 (on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC) [hereinafter "Data Retention Directive"].

often useful in investigating serious crimes.[127] This evidence was subsequently questioned by the independent data-protection officers called upon to examine the proposed directive.[128] Notwithstanding this skepticism, a data-retention requirement of six months to two years was ultimately passed. But what is significant for purposes of this discussion is that the Council of Ministers had to produce some evidence in support of the data processing. It could not simply order the collection of call data based on entirely unsubstantiated speculation that the scheme might accomplish the crime-fighting purposes.

Under the second prong of the proportionality test, the government would have to show that the data-mining program was necessary for protecting national security. In practice, this means that the government would have to refute claims that alternative, less privacy-burdensome programs could accomplish, just as effectively, the same anti-terrorism aims. This issue is directly related to the amount of data collected and the length of time of data retention and therefore will be discussed below, in conjunction with the Council of Europe Convention.

The last part of the proportionality analysis would require the government to demonstrate that the public security ends of the call database outweighed the harm to the privacy right—or, seen from the individual's perspective, that the burden on the right is "proportionate" to the government purpose. This question turns entirely on the magnitude of the harm to the individual right as compared to the benefit to the public interest. When data-mining is conducted for national security purposes, the privacy interest is strong because of the risk that the individual might be wrongly investigated, detained, prosecuted, even convicted. It is stronger than when, say, personal information is used to distribute welfare benefits. The importance of the public interest all depends on what type of suspicion, which types of threats to national security, serve as the trigger for data-mining. In the case of the NSA call-records program we don't know; this is part of the problem for European privacy law. But according to the German Constitutional Court, not all threats warrant intelligence-related searches of telecommunications data: international terrorist attacks, international proliferation of weapons, and the illegal introduction of a not insignificant quantity of narcotics from abroad, yes, international counterfeiting, no.[129] More to the point, the Constitutional Court has recently held that a general fear of terrorism in the wake of September 11 is not good enough to trigger anti-terrorism data-mining.

On April 4, 2006, the Constitutional Court found that police data-mining carried out after September 11 to identify Islamic sleeper cells was unconstitutional.[130] In Germany, anti-terrorism data-mining was first used in the 1970s to fight the Red Army Faction, a left-wing terrorist group. The German version of anti-terrorism data-mining

---

[127] European Data Protection Supervisor Opinion, *supra* note__ at 4.
[128] European Data Protection Supervisor Opinion, *supra* note__ at 4-5; Art. 29 Data Protection Working Party, Opinion 4/2005 of Oct. 21, 2005, p. 6, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp113_en.pdf.
[129] *See* Judgment on G10 Amendments, *supra* note__.
[130] *See* Judgment on Data-mining, *supra* note__.

(*Rasterfahndung*) appears to be technologically less ambitious than the American version.[131] Terrorist profiles are first created, based on characteristics generally believed to be associated with terrorism. Those profiles are used to search public and private databases. This results in a list of individuals who are then subject to examination by the police to establish whether they do indeed pose a threat to public safety. In the wake of September 11, the police forces of the Länder undertook a coordinated effort to collect and search various data sets based on a common terrorist profile: male, age 18–40, student or former student, Islamic faith, citizenship or birthplace in a country with a predominantly Islamic population. (It should be remembered that, in Germany, the police have so-called "preventive" powers to thwart future threats as well as "repressive" powers to investigate crimes that have already been committed.) The results of these searches were transmitted to the Federal Police Office, which matched the names against other data sets, containing information on other characteristics associated with terrorism, and thereby narrowed the pool. The names of suspects were then sent back to the Länder police for further review and possible surveillance and questioning. These activities were authorized by specific provisions of Land police acts that allow the police to collect and analyze data for purposes of state security or for protecting the "life, health, or freedom of a person."

In a complaint brought against the state of North-Rhine Westphalia, the Constitutional Court found that the data-mining program was unconstitutional. The Court reaffirmed its earlier case law on the right of informational self-determination: the right protects against the police's collection, transfer, storage, or processing of personal information.[132] Moving to the proportionality inquiry, the Court found that the national security purpose of the program was legitimate and that the data-mining was a suitable and necessary means of obtaining that goal. But the Court concluded that the burden on the right of informational self-determination was not proportionate to the public ends being pursued. Such data-mining, with such grave consequences for constitutional rights, would only be acceptable if there were actual facts demonstrating an "imminent and specific endangerment" (*konkrete Gefahr)* of a terrorist attack. In this instance, police data-mining had been triggered by a general fear of terrorism following September 11—for the Constitutional Court not reason enough to intrude upon the privacy right.

Now back to European law. At this point, the data-protection inquiry turns to the more specific requirements of the Council of Europe Convention and national laws. Is the call data being used by the government *only* for purposes of identifying possible terrorists and thwarting future terrorist attacks? This is one more difficulty with the secretiveness of the NSA program: no assurances have been given that the call data is not being used for more banal purposes, for instance, for identifying ordinary bank robbers and turning over their names to law enforcement officials.

---

[131] *See* Note from German Delegation to Article 36 Committee on Europe-Wide Computerised Profile Searches, Doc. No. 6403/02, March 8, 2002, available in register of documents of the Council of Ministers of the European Union.
[132] *Id.* at paras. 68-75.

Is the *amount* of data being processed no more than necessary to accomplish the terrorism-fighting purpose? Curiously, at least for a European audience, when certain senators learned of the call database, they complained that it contained too little data—not too much.[133] If the purpose is to foil terrorist plots on American soil, they reasoned, shouldn't the NSA have information on *all* the calls made and received by *all* Americans, not just clients of AT&T and Verizon? But, in Europe, the amount of call data would probably be considered excessive. Again, the debates on the recent EU Data Retention Directive are instructive. Under the Directive, the police may obtain electronic communications data from providers only "in specific cases"[134] and only for purposes of fighting "serious crime."[135] A program giving the government routine, indiscriminate access to *all* traffic data of *all* customers would probably involve an excessive amount of data under European law.[136]

As for the time of data retention, that also would be too long. From the press accounts, it appears that the NSA began collecting call data immediately after September 11, 2001. There does not appear to be any requirement to erase the data. That means that some of the information is over five years old. In the European Union, even the most hawkish of Member States—the United Kingdom, France, Ireland, and Sweden—only pushed for a three-year data retention period, after which call data would have had to be destroyed.[137] Five years is far beyond anything ever imagined for the European Union.

The accuracy requirement would probably be satisfied. Since the purpose of the NSA program is to track individual behavior, not, say, award benefits, it is not critical that the personal data in the system be routinely checked and updated. Call data, moreover, does not generally reveal sensitive personal characteristics such as religious affiliation, and therefore it would not require additional safeguards under European law. It seems safe to assume that the "appropriate security measures" have been adopted. The most technologically sophisticated of all U.S. government agencies has probably taken the necessary steps to protect the call data from unauthorized disclosures.

Individuals, however, have absolutely no right to check on their personal data being used by the NSA. On this last step of the data-protection analysis, European systems differ considerably. Some have made more extensive use of the national security exemption than others. Neither Germany nor France, however, categorically bars individuals from exercising their right of access in cases of national security data processing.

---

[133] *See Lawmakers: NSA database incomplete*, *supra* note__ .
[134] Data Retention Directive, *supra* note__art. 4.
[135] *Id.* art. 1.1.
[136] The Directive, however, only applies to access by national police for "purpose of the investigation, detection and prosecution of serious crime . . ." Data Retention Directive, *supra* note__ art. 1.1. It does not cover access by security services. Therefore the analogy to the NSA program is not exact.
[137] Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection, and prosecution of crime and criminal offenses including terrorism, Council Doc. 8958/04, April 28, 2004, art. 4.

Under German law, access to one's personal data and the correction, erasure, or blocking of such data count as the "inalienable rights of the data subject."[138] National security agencies may, on a case-by-case basis, deny access if disclosure would "impair public safety or order or otherwise be detrimental to the Federation or a Land."[139] Even these agencies, however, must give reasons for denying such a request, either to the individual directly or to the Federal Commissioner for Data Protection, unless giving reasons would itself jeopardise "public safety or order or otherwise be detrimental to the Federation or a Land."[140] The federal police, by contrast, are never exempted from their duty to give access, although the information may be communicated to the Federal Data Protection Commissioner rather than to the individual.[141] Land regulation of their police forces varies but the Hessian legislation is illustrative. The Hessian police are not given a blanket exemption from disclosure. Rather, the Hessian Data Protection Law states that the statutory provisions on access

> shall not apply where after balancing the rights accorded to the data subject against public interest in data secrecy . . . the latter interests prevail. The decision shall be made by the head, or his designated deputy, of the data storage agency. If the data subject is denied information or the right to inspect records, he shall be informed of the major reasons on which the denial is based and of his right to complain to the Hessian Data Protection Commissioner.[142]

Under the French data-protection law, the right of access "where processing involves State security, defence or public safety" is indirect, meaning that an individual cannot approach the intelligence agency directly but must proceed via CNIL, the independent privacy commission.[143] The procedure for so-called "indirect access" is as follows:

> The commission [CNIL] receives the access request and appoints one of its members, who is or has been a member of the "Conseil d'Etat" [highest administrative court], the "Cour de Cassation" [highest civil court] or the "Cour des Comptes" [independent body responsible for auditing government accounts], to carry out the necessary investigations and have the necessary modifications made. An officer of the commission may assist the appointed member of the commission. The applicant shall be informed that the verifications have been carried out.
>
> Whenever the commission establishes, with the agreement of the data controller, that the disclosure of the data does not undermine its purposes,

[138] Federal Data Protection Act § 6.
[139] Federal Data Protection Act § 19(3).
[140] Federal Data Protection Act §§ 19(5), 19(6). In the case of telecommunications data, this procedure would be handled by the G10 Commission.
[141] Federal Data Protection Act § 6 (2).
[142] Hessian Data Protection Act § 18(5).
[143] Law no. 78-17, art. 41.

> State security, the defence or public safety, these data may be disclosed to the applicant.

By contrast, the default rule for personal data held by law enforcement agencies is direct access. The regulation authorizing the data processing, however, may provide for indirect access:

> The [right of indirect access] shall apply to processing carried out by public authorities and departments and private legal entities entrusted with a public service mission for the prevention, investigation or proof of criminal offenses, or the assessment or collection of taxes, where the [authorizing regulation] provides for this right.

In sum, notwithstanding all of the exceptions for national security and law enforcement, the NSA call database would violate this European right, too.

The principal institution of European privacy law—an independent watchdog agency—is also missing in the United States.[144] The NSA did not first consult an independent privacy agency before undertaking the call-records program. In France or Germany, by contrast, a government proposal for data-mining, even intelligence-related data-mining, would have to be submitted to an independent privacy regulator for review.[145] Such review would entail a wide-ranging proportionality analysis—along the lines of this article—and would result in a finding on the lawfulness of the program, as well as recommendations for limiting the government's interference with the right to privacy.[146] This institutional requirement is designed not only to improve the privacy quality of the program by ensuring that the necessary safeguards are in place to prevent

---

[144] This is a slight oversimplification. The Computer Matching and Privacy Protection Act of 1988 requires that each agency create a "data integrity board," entrusted with overseeing privacy in computer matching projects. 5 U.S.C. § 552a(p). However, the members of such boards are appointed by the agency head and their mandate is limited. The Department of Homeland Security has a privacy officer, but, again, the privacy officer is appointed by the administration and therefore is not independent. Homeland Security Act of 2002, § 222, Pub. L. No. 107-296, 116 Stat. 2135 (2002), codified as amended at 6 U.S.C. § 101 et seq**.** Moreover, she only has jurisdiction over the activities of the Department of Homeland Security and her powers are limited.

[145] *See* Law no. 78-17, art. 11(4) (general duty to consult CNIL on "any bill or draft decree relating to the protection of individuals in relation to automatic data processing"); arts. 11(2)(a) & 26 (specific duty to obtain "reasoned and published" opinion of CNIL on ministerial order (*arrêté*) authorizing "the processing of personal data carried out on behalf of the State and: (1) which involves State security, defence or public safety; or (2) whose purpose is the prevention, investigation or proof of criminal offences, the prosecution of offenders or the exception of criminal sentences or security measures."); Federal Data Protection Act §§ 26 (2), 26(3) (general power of Federal Data Protection Commission to give opinions and recommendations on government measures); Hessian Data Protection Act §§ 24(1), 25, 29 (duty to inform Hessian Data Protection Commissioner of "new procedures and techniques in data processing as well as of any preliminary draft proposals on the automated processing of personal data" and power to give opinions and recommendations).

[146] *See, e.g.*, CNIL, Decision no. 2005-208, Oct. 10, 2005, http://www.cnil.fr/index.php?id=1883&delib[uid]=75&cHash=23d7fc2011 (opinion on law authorizing various types anti-terrorism surveillance, including government access to telecommunications and airline data).

against government abuses. Scrutiny by an independent regulator also improves public awareness of government intrusions in highly technical policy areas, policy areas in which the burden on privacy can be obscure to the average citizen. In sum, the involvement of a privacy agency, coupled with the requirement of a detailed, accessible authorizing law, gives rise to a vigorous public debate on the privacy costs of government initiatives that may—or may not—be necessary in a post-September 11 world.

A European privacy agency would also have the power to make sure that intelligence officers running a data-mining program were complying with basic privacy safeguards. In France, this takes the form of a standard administrative enforcement scheme: CNIL has the power to inspect government programs,[147] and, if it finds violations, to impose sanctions.[148] In data processing related to national security and law enforcement, those powers are quite soft, but they exist nonetheless. Data processing related to "state security" can be insulated from CNIL's inspection powers at the time that the program is authorized.[149] If CNIL learns of privacy breaches in government programs involving "state security" or "criminal offenses," it has the power to issue warnings and to order the termination of such breaches. If the order is ignored, CNIL may publicize the privacy breach. When the violation of privacy rights is "urgent," CNIL has the power "notify the Prime Minister so that he may, if necessary, take measures to stop the violation . . . The Prime Minister shall inform the commission of the steps he has taken within fifteen days of receiving the notification."[150] And in the case of a "serious and immediate" violation, CNIL's chairman may "ask, in summary proceedings, the competent jurisdiction to order, if necessary applying a daily penalty, any security measure necessary for the protection of these rights and liberties."[151] Finally, private actors and public officials may be criminally prosecuted under the French data-protection law.[152]

In contrast with the French system of privacy enforcement, the German system relies more on consultation and persuasion than on hard sanctions. This is also the case when data processing is conducted for intelligence and law enforcement purposes. Thus, in Germany, each public and private body—including intelligence agencies— must appoint an internal "data-protection official" responsible for overseeing compliance within the organization.[153] Internal data-protection officials must notify the responsible data-protection agency of any violations. The Federal Data Protection Commissioner is responsible for "monitor[ing] compliance"[154] and the Land authorities for "monitor[ing] implementation"[155] within their respective jurisdictions. Thus, in the case of a suspected privacy violation by an agency like the Federal Intelligence Service, the Federal Commissioner would have the power to inspect documents, to obtain answers to

---

[147] Law no. 78-17, art. 44.I.
[148] *Id.* art. 45.I.
[149] *Id.* art. 44.IV.
[150] *Id.* art. 45.II(3).
[151] *Id.* art. 45.III.
[152] *Id.* art. 50.
[153] Federal Data Protection Act §§ 4f-4g.
[154] *Id.* § 24(1).
[155] *Id.* § 38(1).

questions, to advise on steps for improving data protection, and, in the case of a breach, to file a complaint with the head of the agency and to require a response from that agency, outlining the agency's remedial measures.[156] Should compliance not be forthcoming, the Federal Commissioner is authorized to report the matter to Parliament.[157] This is the standard operating procedure for monitoring all agencies. Data-protection commissioners in the Länder, responsible for overseeing their government administrations, including their police forces and domestic security agencies, have similar powers of inspection and persuasion.[158]

Only two exceptions are made for intelligence and law enforcement agencies. First, inspections must be conducted by the Federal Commissioner in person or by assistants specially designated by him.[159] Second, when the agency is a federal intelligence agency and the personal data is telecommunications data, as in our hypothetical, primary responsibility for oversight rests with the parliamentary G10 Commission.[160] The Federal Commissioner may be requested by the G10 Commission to investigate and report on such data processing, but he does not have independent powers. The same is the case when the agency is a Land intelligence agency and the personal data is telecommunications data—oversight is the task of the Land parliament, not the Land data-protection commissioner.[161]

The last aspect of the NSA episode that is puzzling to the European observer is the availability of so much personal data in the hands of private firms, ready to be transferred to the government whenever it so requests. As explained earlier, European data-protection law covers both the public and private sectors. To collect personal data, private actors must have a legitimate purpose and must use such data only in accordance with a legitimate purpose. For commercial operators, the legitimate purpose is generally providing a good or service to customers and collecting the payment due for the good or service. Only personal information relevant to this contractual relationship can be gathered. And once the contract has been fulfilled—the good or service provided and the payment rendered—the personal data is to be erased. It cannot be kept and used for other purposes. The most common American counterexample—aside from helping out the NSA—is using personal data collected for a contractual relationship to market unrelated goods and services.

Providers of electronic communications services are not only governed by these general principles of European law. For them, there is a specific EU law requiring that a subscriber's communications data be erased once no longer necessary for connecting the

---

[156] *Id.* §§ 24, 25.
[157] *Id.* § 26.
[158] *See, e.g.*, Hessian Data Protection Act §§ 27, 29, 30.
[159] Federal Data Protection Act § 24(4).
[160] *Id.* § 24(2).
[161] E-mail from Alexander Dix, Berlin Commissioner for Data Protecton and Freedom of Information (Oct. 6, 2006) (on file with author).

communication or for obtaining payment on the bill.[162] The law allows for some exceptions: if the subscriber gives his or her consent at the time of signing up for the service, the provider may use the subscriber's personal information for purposes of marketing additional services.[163] Member States may require, by law, that their electronic communications providers retain subscriber data and make that data available for legitimate government purposes.[164] Such data retention requirements have been enacted in most Member States to enable their police forces and intelligence agencies to obtain communications data necessary for their investigations. As a matter of fact, the EU Data Retention Directive was designed to harmonize some of these very different data retention requirements at the Member State level.[165] In Europe, therefore, telecommunications providers do keep personal data to assist with intelligence and police operations, much as AT&T and Verizon kept the call records that were later transferred to the NSA. But, unlike their American counterparts, European telecommunications providers can keep personal data after performance on a subscriber contract only because specific laws instruct them to do so, setting down the type of data to be retained, the time when the data must be erased, and the conditions under which the data may be requested by government agencies.

V. THE CONSEQUENCES OF COMPARISON

A. Obstacles to Transatlantic Cooperation on Fighting Terrorism

The practical consequences of these legal differences are dramatic. Transatlantic cooperation on national security has already been strained by differences in privacy law. The latest string of revelations related to the NSA's activities can only make cooperation more difficult. The U.S. government might wish to obtain information held by European spy and law enforcement agencies for purposes of preventing terrorist attacks. Yet because the way it handles personal data is so out-of-line with European law, it is increasingly unlikely that it will be able to get that data.

The dilemma for any European government is simple: how can it transfer information on its citizens to the U.S. government when, in all likelihood, the information will end up in a database that would clearly be unlawful if created by that same European government—especially when the information might be used, at some future point in time, to wrongly detain, prosecute, convict, even execute a European citizen? This reluctance is not simply a matter of moral scruples or political survival. In many European countries, it is the law of data protection. The government can transfer personal data only to countries with an "adequate" level of data protection. And by this

[162] Directive 2002/58/EC of the Eur. Parl. and of the Council of 12 July 2002 (concerning the processing of personal data and the protection of privacy in the electronic communications sector), 2002 O.J. (L 201) 37, art. 6.
[163] *Id.* art. 6.3.
[164] *Id.* art. 15.1.
[165] *See supra* note__ and accompanying text.

point it should be clear that the United States would not count as one of those countries.[166]

The legal obstacles to exchanging intelligence merit further exploration. On this issue, European law is mostly national. On the subject of third countries, the Council of Europe Convention has little to say.[167] Unfortunately, national laws vary even more than the usual in their treatment of third-country transfers for national security and law enforcement purposes. Both the German and French data-protection laws, however, impose blanket bans on transfers to inadequate third countries; they create such limited exceptions to those bans that the routine exchange of intelligence with an inadequate country would be prohibited.

In the German law

> transfer [of personal data] to foreign [non-EU], supranational or international bodies . . . shall not be effected in so far as the data subject has a legitimate interest in excluding transfer, in particular if an adequate level of data protection is not guaranteed. . . .[168]

The only exception to this prohibition is national defense or certain duties under international law:

> [The prohibition] shall not apply if transfer is necessary in order to enable a public body of the Federation to perform its duties for compelling reasons of defence or to discharge supranational or international duties in the field of crisis management or conflict prevention or for humanitarian measures.[169]

---

[166] The adequacy of U.S. law for purposes of EU personal data transfers has been object of extensive study. *See, e.g.*, Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1 (2000); Commission Decision 520/2000/EC, 2000 O.J. (L 215) 1. The focus, however, has been on the adequacy of private sector—not public sector—data-protection law. This is because the only EU (as opposed to national) adequacy requirement applies to market-based transfers of personal data, not to transfers related to government policing or national security. *See* Council and Eur. Parl. Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, *supra* note__art. 25. As the European Court of Justice has recently held, third-country transfers of personal data to assist with law enforcement or national security fall outside the scope of EU data-protection law. Joined Cases C-317/04 and C-318/04, European Parliament v. Council, paras. 55-59 (May 30, 2006).

[167] A protocol to the Convention, signed in 2001, would require the parties to allow transfers to third states only if such states provided an "adequate level of protection." *See* Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows, Nov. 8, 2001, E.T.S. No. 181. As of August 2006, however, this protocol had been ratified by only thirteen countries. Moreover, the parties are allowed to derogate from the adequacy requirement for a number of reasons including a "legitimate prevailing interest, especially important public interests."

[168] Federal Data Protection Act § 4b(2).

[169] *Id.* § 4b(2).

To obtain personal data, the U.S. government would have to argue that the data involved a security threat to *both* Germany and the United States and that, as a result, the transfer would advance the purpose of defending Germany from foreign attack. The only other avenue available to the U.S. government would be an agreement with Germany promising that it will treat personal information in accordance with the basic principles of German privacy law. The German data-protection law directs officials to assess adequacy "in the light of all circumstances surrounding a data transfer operation or a category of data transfer operations."[170] An international agreement would count as one of those circumstances.

Likewise, under the French data-protection law, personal data may not be transferred to a state outside the European Union if that state "does not provide a sufficient level of protection of individuals' privacy, liberties and fundamental rights with regard to the actual or possible processing of their personal data."[171] There are a number of exceptions to this prohibition, the most relevant to intelligence-gathering being a determination that a particular transfer would serve "the protection of the public interest."[172] Moreover, when personal data processing "involves State security, defense, or public safety"[173] or "whose purpose is the prevention, investigation, or proof of criminal offences, the prosecution of offenders or the execution of security sentences or security measures"[174] transfers to inadequate third countries may be authorized by special government decree.[175] Before promulgating such a decree, however, the government, must solicit the opinions of the CNIL and the Conseil d'Etat (France's highest administrative body).[176] The government must also be convinced that privacy rights will be afforded a "sufficient level of protection" in the receiving country.[177] Under French law, therefore, routine exchanges of intelligence-related personal data with the United States can only occur upon a finding of a "sufficient level of protection." Given the numerous discrepancies between the two systems of data privacy, such a finding could only occur through an international agreement of the kind discussed in relation to Germany.

In addition to German, French, and other national laws, a measure under negotiation in the European Union, once finalized, might also create difficulties for

---

[170] *Id.* § 4b(3).
[171] Loi 78-17, art. 68.
[172] *Id.* art. 69(2).
[173] *Id.* art. 26.I (1).
[174] *Id.* art. 26.I (2).
[175] *Id.* art. 69. In 2003, a law was enacted to improve internal security. Among its many provisions, the law specifically addressed exchanges of personal data between the French police and foreign police. It too requires adequacy before such exchanges may occur. Law No. 2003-39 of March 18, 2003, Journal Officiel de la République Française [J.O.] [Official Gazette of France], March 19, 2003, p. 476, art. 24 ("Les données contenues dans le traitement automatisés de données personnelles gérés par les services de police et de gendarmerie nationales peuvent être transmises à . . . des services de police étrangers qui présentent, pour la protection des données personnelles, des garanties equivalentes à celle du droit interne, dans le cadre des engagements internationaux régulièrement introduits dans l'ordre juridique interne. ").
[176] Loi 78-17, art. 69.
[177] *Id.*

information-exchange with the United States.[178] In this instance, the main impact would be on personal data sought to investigate past crimes or to prevent imminent offenses, a matter more for law enforcement agencies, i.e., the FBI in its law enforcement guise, than a national security agency like the NSA. Since the early 1990s, the European Union has become increasingly active in promoting cooperation on criminal matters among national police forces, prosecutors, and criminal courts. To ensure that different levels of privacy protection do not make national authorities reluctant to exchange personal information amongst themselves, a Framework Directive is being negotiated that would set down common data-protection standards for all European authorities responsible for "preventing and combating crime."[179] Under the latest available draft, information sent by one Member State to another may not be transferred onwards to a third country unless consent to the transfer has been given by the original Member State *and* an adequate level of data protection exists in the third country.[180] The only caveat to the adequacy requirement is for transfers "if absolutely necessary in order to safeguard the essential interests of a Member State or for the prevention of imminent serious danger threatening public security or a specific person or persons."[181] As in the German and French laws, an international agreement with a third country, stipulating the conditions under which data will be processed, can constitute grounds for an adequacy finding, even if the country's domestic privacy law is unsatisfactory. Again, therefore, an international agreement would be the only way in which the U.S. government could obtain routine access to European personal data.

A number of bilateral agreements do allow for information exchange between Europe and the United States. These agreements, known as treaties on mutual legal assistance (MLAT), guarantee access to information in connection with criminal investigations.[182] Police authorities in one state may request from the police authorities in another state public or private records located in that state. MLATs, however, are not particularly useful to the American intelligence community. Under the terms of MLATs, before a state may request information on an individual, it must show that the individual is suspected of a crime or has been charged with a criminal offense. In other words, MLATs cover only criminal investigations, not national security programs designed to ward off future threats.[183]

---

[178] Note from President to Multidisciplinary Group on Organised Crime on "Proposal for a Council Framework Directive on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters," Brussels, June 23, 2006, Doc. No. 6450/5/06 REV 5.
[179] Consolidated Version of the Treaty on European Union, art. 29, 2002 O.J. (C325) 1, 21.
[180] Proposal for a Council Framework Directive, *supra* note__art. 15.1.
[181] *Id.* art. 15.6.
[182] *See, e.g.*, Treaty on Mutual Legal Assistance in Criminal Matters Between the United States of America and France, Senate Treaty Doc. 106-17, art. 1 (entered into force December 1, 2001) [hereinafter "U.S.-Fr. MLAT"]; Treaty Between the United States of America and the Federal Republic of Germany on Mutual Legal Assistance in Criminal Matters, Senate Treaty Doc. 108-27, art. 1 (signed Oct. 14, 2003 but not yet in force [hereinafter "U.S.-F.R.G. MLAT"].
[183] *See* U.S.-F.R.G. MLAT art. 1; U.S.-Fr. MLAT art. 1; Agreement on Mutual Legal Assistance Between the European Union and the United States of America, 2003 O.J. (L 181) 34, arts. 4.1(b), art. 8 (signed June 25, 2003 but not yet in force) [hereinafter "U.S.-EU MLAT"].

MLATs have another limitation: they contain numerous exceptions to the duty of cooperation. Many, including the French and German ones, do not require states to assist with requests for government records; such assistance is left to the requested state's discretion.[184] Furthermore, a state is allowed to deny a request for assistance or to attach conditions to such a request if "execution of the request would prejudice the sovereignty, security, public order, or other essential interests" of that state. Data protection would count as one of those essential interests, hence preventing cooperation. A recently negotiated MLAT between the European Union and the United States is specifically directed at removing the data-protection impediment: it would bar European countries from routinely invoking data protection as grounds for denying U.S. requests for assistance.[185] But because of this and other provisions, it is uncertain that the MLAT will be ratified on the European side. Many argue that, without guarantees from the United States, this provision would breach European human rights law.[186]

Recently, the U.S. government has sought to move beyond information for criminal investigations and to obtain European personal data in connection with national security operations. Compared to criminal investigations, vastly more information is needed to ascertain whether vague suspicions of possible, future harms have some basis in fact or must be dismissed. It should come as no surprise, therefore, that agreement on this type of information-exchange has been even more elusive than in the area of criminal investigations.

To date, the principal example of this type of transatlantic cooperation—or, more accurately, transatlantic fractiousness—is the transfer of European airline-passenger data to the U.S. government.[187] After September 11, the U.S. Bureau of Customs and Border Protection (CBP) began demanding access to European airline-passenger data well before European airplanes took off from European airports to land in the United States. Part of the purpose was quite innocuous: to check for suspected terrorists and to require that they be stopped from boarding planes bound for the United States. But the other purpose—and the associated privacy risks—raised red flags for the European authorities: the data was to be used to identify individuals requiring surveillance while in the United States, either immediately or at a future time if their subsequent behavior gave rise to a suspicion of criminal activity. The method by which the passenger data was to be transferred to the CBP was through a so-called pull system: CBP was to have direct access to the data contained in the airline-passenger systems of European carriers—systems located in Europe, not the United States. This clearly constituted an extraterritorial exercise of regulatory jurisdiction by the United States. But airplanes, of course, must eventually land in the United States, at which point they come squarely within the reach of U.S. jurisdiction. Practically speaking, this meant that if the airlines failed to cooperate with

---

[184] U.S.-F.R.G. MLAT art. 9; U.S.-Fr. MLAT art. 20.

[185] U.S.-EU MLAT art. 9.2(b) ("Generic restrictions with respect to the legal standards of the requesting State for processing personal data may not be imposed by the requested State as a condition under subparagraph (a) to providing evidence or information.")

[186] *See, e.g.*, Select Committee on the European Union, Report, 2002-03, H.L. 38, at 14, para. 35 (report on EU/US Agreements on Extradition and Mutual Legal Assistance).

[187] *See* Francesca Bignami, *Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network*, 26 MICH. J. INT'L L. 807, 863-65 (2005).

CBP's earlier demands, entry of their passengers to the United States could be denied or delayed and civil fines could be imposed.

Notwithstanding these enforcement tools, European airlines did not accede to U.S. demands immediately. Why wasn't cooperation forthcoming? This is even more surprising given that the punitive measures were actually imposed in some instances: passengers on European carriers were sometimes stuck for hours on U.S. runways, waiting to be allowed entry into the United States. The airlines didn't cooperate for some of the same reasons that the transatlantic exchange of personal data between spy and police agencies has been so difficult: under European law, such transfers would have to be authorized by a specific piece of regulation and could not occur absent a finding of the adequacy of the data-protection guarantees in the receiving country. In other words, by satisfying the demands of the U.S. government, the airlines would be breaking European law. The airlines, faced with this dilemma, went to the European Commission seeking action that would allow them to operate their transatlantic flights in compliance with the law on both sides of the Atlantic. It took almost three years of diplomatic wrangling for the United States and the European Union to come to an understanding: in spring 2004 the two sides signed an agreement, specifying the type of passenger data that could be gathered from European airline reservation systems and the conditions under which it would have to be handled.[188]

These are the terms: CBP is allowed access to thirty-four—out of thirty-nine—fields contained in airline reservation systems under an individual's passenger name record (PNR) number. This includes the individual's address, email address, telephone number, travel itinerary, round-trip or one-way ticket purchase, and payment information. If the information is never manually accessed, it must be erased after three-and-a-half years; otherwise it must be erased after eight years, with an exception for information that was used in a government investigation.[189] The purposes for which the personal information may be used are limited to "preventing and combating" the following crimes: terrorism and related crimes; other serious crimes—including organised crime—that are transnational in nature; and flight from warrants or custody for those crimes.[190] CBP is barred from processing personal data considered, under European law, to be "sensitive data."[191] Only CBP may access the data on a routine basis; CBP may transfer European passenger data to other law enforcement and counter-terrorism agencies but only if it first determines that transfer of a particular passenger's data would further the crime-fighting purposes outlined earlier.[192] Those government agencies are held to the same standards

---

[188] *See* Commission Decision 2004/535/EC of 14 May 2004 on Adequate Protection of Personal Data Contained in the Passenger Name Record of Air Passengers Transferred to the United States Bureau of Customs and Border Protection, 2004 O.J. (L 235) 11; Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, 2004 O.J. (L 183) 83.
[189] Undertaking of the Department of Homeland Security Bureau of Customs and Border Protection (CBP), para. 15 *in* Commission Decision 2004/535/EC, 2004 O.J. (L 235) 11, Annex.
[190] *Id.* para. 3.
[191] *Id.* paras. 9-11.
[192] *Id.* paras. 28-30.

as CBP, including the restrictions on information-sharing with other government agencies.[193] Passengers are guaranteed access to their personal information under the Freedom of Information Act.[194] Finally, the Chief Privacy Officer of the Department of Homeland Security is recognized as exercising many of the same oversight functions as independent privacy agencies in Europe.[195]

From the perspective of European privacy advocates, this agreement was far from satisfactory. However, it did render unlawful the kind of data-mining and data-sharing conducted as part of government programs like the NSA call database. But after only two years of operation, it appeared that the PNR agreement might unravel. On May 30, 2006, the European Court of Justice found the PNR agreement to be unlawful under European law. The grounds for the Court's judgment had nothing to do with privacy. In fact, the Advocate General's opinion that preceded the Court's judgment had found that the agreement respected fundamental human rights guarantees on data protection.[196] Rather, the Court found that the European Commission and the Council had exceeded their jurisdiction because they had concluded the agreement under the common market pillar when the purpose of the data transfers was not to facilitate trade, but to prevent and investigate crime.[197] Therefore, the European Union announced to the United States on July 3, 2006 that it was withdrawing and, on September 30, 2006, the agreement terminated.[198]

The big question following the Court of Justice's decision was what, if anything, would replace the PNR agreement. On the European side, the strategy was to sign an identical agreement between the same parties (the United States and the European Union, not individual European countries as some had suggested) just under the correct pillar covering criminal matters. By the time the negotiations were concluded on October 6, 2006, however, it was clear that this ambition had not been realized.[199] The current agreement, which still must be signed and ratified by the Council, relies on the data-protection undertakings entered into by the U.S. government in 2004 as part of the first round of negotiations. The undertakings implemented into U.S. law the terms of the PNR agreement based on the Department of Homeland Security's statutory authority. These undertakings remain in effect. But they have been undermined by a new Letter of Interpretation that sets out how the Department of Homeland Security (DHS), CBP's parent agency, will interpret the undertakings. In the Letter of Interpretation, DHS states that European passenger data may be shared with all agencies exercising counter-

---

[193] *Id.* paras. 31-32.
[194] *Id.* para. 37.
[195] *Id.* paras. 31, 41, 42.
[196] Opinion of Advocate General Léger, Joined Cases C-317/04 and C-318/04, European Parliament v. Council (Nov. 22, 2005).
[197] Joined Cases C-317/04 and C-318/04, European Parliament v. Council (May 30, 2006).
[198] *See* Note from Presidency to Coreper/Council on Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security, Doc. No. 13668/06, Oct. 6, 2006, available in register of documents of the Council of Ministers of the European Union, http://www.consilium.europa.eu.
[199] *See id.* paras. 5-6, p. 2.

terrorism functions, without any showing that such data is relevant to a specific investigation;[200] that all the data contained in European passenger records systems may be requested, not only the thirty-four items specified in the undertakings;[201] and that the data may be retained indefinitely.[202]

A similar set of demands for European personal data have been made on the banking industry. In summer 2006, it was revealed that ever since September 11, the Society for Worldwide International Financial Telecommunication (SWIFT) has been transferring massive amounts of data on international bank transfers to the U.S. Department of the Treasury.[203] SWIFT is a cooperative, established under Belgian law, of financial institutions located throughout the world. It runs a network designed to execute international bank transfers. It has two operations centers, one in Europe and one in the United States. All messages ordering payments between banks are stored, in duplicate, at these two operations centers for 124 days. After September 11, the U.S. Treasury Department began issuing administrative subpoenas for the data held in SWIFT's U.S. operations center. These administrative subpoenas are known as National Security Letters and can be used to obtain information in investigations to protect against international terrorism.[204] In SWIFT's case, the subpoenas were drafted broadly, ordering the production of information on transactions involving certain countries over extended periods of time.[205] Although the precise figures are secret for national security reasons, according to one report the data transferred to the Treasury Department in any give year could very well count all the messages sent via the SWIFT system, which in 2005 numbered 2,518,290,000.[206]

After this came to light, a number of European data-protection authorities called for action. Since much of the transactional information came from Europe, it was clear to all concerned that European privacy law was triggered. In fact, from the beginning, SWIFT knew that it was running the risk of violating European privacy law: it requested and received a "comfort letter" from the Department of Treasury in which the Department pledged to support SWIFT in the event that it was later sued by foreign governments or third parties.[207] The Belgian Data Protection Commission took the lead in the investigation since, under European data-protection rules, it is the privacy agency with the strongest claim of jurisdiction over SWIFT. In fall 2006, the Belgian Commission categorically condemned SWIFT—and indirectly the U.S. government. It is worthwhile repeating the Belgian Commission in full:

---

[200] *See id.* annex 3, p. 12.
[201] *See id.* annex 3, p. 13.
[202] *See id.* annex 3, p. 14.
[203] *See* Belgian Data Protection Commission, Opinion No. 37/2006 of 27 September 2006 on the transfer of personal data by the CSLR SWIFT by virtue of UST (OFAC) subpoenas (non-official and temporary translation), http://www.privacycommission.be/communiqués/opinion_37_2006.pdf.
[204] *See supra* note__ and accompanying text.
[205] *Id.* at 5/27
[206] *Id.* at 6/27.
[207] *Id.* at 6/27.

> Considering that the recipient of the data (US Treasury) was never subjected to an appropriate level of protection in accordance with article 21 of the Belgian Data Protection Law and the EU Directive, the Commission is of the opinion that SWIFT violated . . . [the Belgian Data Protection Law]. It can be considered a serious error of judgement on the part of SWIFT to subject a mass quantity of personal data in a secret and systematic manner for years to the surveillance of the US Treasury without at the same time informing the European authorities and the Commission in order to reach a solution under Belgian and European law.[208]

Although it is too early to tell with the bank-transfer data, in the case of airline-passenger data it does not appear that Europe has been able to exert much leverage over the United States. The state control over territory that has served traditionally as the basis for regulatory jurisdiction also influences which approach to privacy will prevail, American or European.[209] European airlines wish to do business with the United States. To do so, they must land and deplane their passengers at U.S. airports. To enjoy this privilege, European carriers are forced to comply with the U.S. government's requests for personal information. And Europe has few carrots or sticks to use in negotiating privacy guarantees for such information. A European privacy authority might threaten to bring prosecutions in its national courts against both European and American airlines for complying with CBP's information requests. But such prosecutions against national carriers would be difficult as a matter of domestic politics and the same prosecutions against American airlines would risk triggering retaliation from the American side.

The relative power of the United States and Europe in this type of situation suggests that the outcome of the SWIFT episode will be similar. To process transatlantic bank transfers, bank orders must be sent from Europe to the United States where, for good business reasons, they are stored for a certain period of time. Because the bank orders are in storage on American territory—and because SWIFT has significant economic assets in the United States associated with such storage—it is easy to compel compliance with any government order. Again, the European Union has few tools to pressure the United States to adopt better privacy guarantees. As a cooperative with a significant European membership, a suit against SWIFT would encounter the same domestic opposition as a suit against a European airline. A European government might go after the financial institutions that are part of the cooperative, some of which are undoubtedly American, but that would carry all the same political risks as suing American airlines.

Another episode of transatlantic discord—involving personal data of particular value to the intelligence community—illustrates the different outcome when the territorial advantage is held by the Europeans. This time, the Americans sought access to

---

[208] *See id.* at 26-27/27.
[209] *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 204 (1987).

the information on transnational crime contained in Europol's central database.[210] Because the two sides were so bitterly divided over data protection, the terms under which access would be permitted had to be negotiated in stages. First came an agreement, signed on December 6, 2001, on the exchange of strategic and technical information on matters such as the routes used by smugglers.[211] This was followed, a full year later, by an agreement on the exchange of personal data.[212] This second agreement requires that requests for information be made in writing and that such requests "provide a concise statement identifying the authority making the request, the matter under consideration, the reason for the request, and the nature of the assistance sought."[213] Such requests must be made in connection with "specific" criminal offenses or for "specific" analytical purposes.[214] The agreement therefore does not contemplate wholesale access to information contained in the Europol database as has been achieved in the case of airline-passenger reservation systems. Most importantly, the parties retain full discretion to deny such requests for personal information and they may subject disclosure to various conditions, including privacy guarantees.[215] The difference in privacy laws has effectively prevented the United States from obtaining routine access to the vast reservoir of information on transnational criminal activity held by Europol. Once, as is planned, the Europol and Schengen systems are merged, that pool of information will become even more extensive.

Thus the transatlantic difference persists, notwithstanding the burden on business and the interest of the U.S. government in obtaining more European police data to better fight crime and terrorism. This outcome defies predictions of regulatory convergence in some quarters. A couple of years ago, Gregory Shaffer observed that U.S. privacy standards were being "ratcheted up" to the level of data protection afforded under European law.[216] Shaffer argued that the logic of trade, reinforced by non-governmental advocacy networks, had produced this phenomenon and would continue to do so. Building on the work of David Vogel and others, Shaffer found that American firms that did business in Europe had an incentive to adopt the higher, more restrictive European privacy standard for all of their business, including their non-European operations. This they accomplished by self-regulation and by putting pressure on their American regulators to adopt standards that were compatible with the European ones. At the same time, because data privacy is a policy problem characterized by externalities, Shaffer hypothesized that European regulators would seek to influence foreign jurisdictions: data

---

[210] For Europol's internal data-protection rules, see Council Act of 3 November 1998 adopting rules applicable to Europol analysis files, 1999 O.J. (C 26) 1.
[211] Agreement Between the United States of America and the European Police Office, arts. 2 & 3, http://www.europol.eu.int/legal/agreements/Agreements/16268-2.pdf.
[212] Supplemental Agreement Between the Europol Office and the United States of America on the Exchange of Personal Data and Related Information, http://www.europol.eu.int/legal/agreements/Agreements/16268-1.pdf. This agreement was signed on December 12, 2002. *See* Europol, Annual Report 2003, point 22, http://www.europol.eu.int/index.asp?page=publar2003#USA.
[213] Supplemental Agreement Between the Europol Office and the United States of America on the Exchange of Personal Data and Related Information, *supra* note __art. 4.
[214] *Id.* art. 5.1.
[215] *Id.* art. 5.4.
[216] *See* Shaffer, *Globalization and Social Protection*, *supra* note__.

can be sent abroad in seconds, at which point privacy is at the mercy of foreign laws and regulators. In Shaffer's account, these forces of globalization have combined with the advocacy efforts of privacy rights groups to produce higher privacy standards in the United States.

There certainly is good evidence for Shaffer's claims. The more recent experience, however, shows the limits of the argument. Even when the economic interests of big players in the global marketplace are at stake—airlines and banks—a strong, countervailing regulatory policy will trump the trade interest in convergence. In this instance, that opposing policy interest is government access to information to assist with law enforcement and national security. Furthermore, when an activity is entrusted to state—not private—actors, the pressure to develop a single modus operandi applicable in all jurisdictions is significantly lower. Policing and national defense are the prime examples of activities handled by government actors, not private firms. And the resistance to convergence of such actors is evident in the continuing difference in how police and spy agencies handle personal data in the United States and Europe: this difference persists even though a relatively small policy shift on the American side would produce significant advantages in the form of easier access to personal data—on, say, Islamic extremists in places like Germany and France.

B. Understanding American Privacy Law

1. The Comparative Method

In some ways, this article is a conventional exercise in comparative law. It takes a presumed problem—safeguarding privacy in the face of government programs like the call-records program—and explores the solutions to that problem in two different legal systems. The so-called "functionalist" method has been employed in countless pieces of individual comparative law research.[217] It has also served as the framework for a number of well-known collaborative projects, including the Rudolf Schlesinger's project on the formation of contracts[218] and the Common Core Project being run out of the University of Trento, Italy.[219]

On the details of the functionalist method, this collaborative work is especially revealing. Research design in such enterprises must be made particularly explicit at the outset, to guarantee that the results will be cumulative and will be able to serve as the basis for more general conclusions. The starting point is a factual hypothetical, abstracted as much as possible from the law of any one country. Scholars from different legal systems are then asked how their system would handle the problem: how would a judge decide the case, based on which rules, general principles, doctrinal reasoning, and, if relevant, rules and institutions outside that particular subject area, such as civil

---

[217] *See generally* Ralf Michaels, *The Functional Method of Comparative Law*, *in* THE OXFORD HANDBOOK OF COMPARATIVE LAW (Mathias Reimann & Reinhard Zimmermann eds., forthcoming 2006), *available at* eprints.law.duke.edu/archive/00001249.

[218] Rodolfo Sacco, *Legal Formants: A Dynamic Approach to Comparative Law*, 39 AM. J. COMP. L. 1, 27-28 (1991).

[219] Vernon Valentine Palmer, *From Lerotholi to Lando: Some Examples of Comparative Law Methodology*, 4 GLOBAL JURIST FRONTIERS 1, 16 (2004).

procedure and constitutional law. Those answers are then synthesized, to discern the extent of commonality and difference among the many legal systems.

An example from the Common Core's study on "Pure Economic Loss in Europe" will illustrate:

> Case 1
>
> While maneuvering his mechanical excavator, an employee of the Acme Road Works cuts the cable belonging to the public utility which delivers electricity to Beta Factory. The unexpected black-out causes damage to machinery and the loss of two days production. Beta Factory's owner claims compensation from the excavator (Acme) not only for the damage to his machinery but also for the damage caused by the loss of production.

Whether and for what reasons Beta Factory would be able to recover for loss of production, together with a number of other hypotheticals, were analyzed by scholars from thirteen different legal systems.[220] Their country reports, together with a synthesis report and a historical chapter, were published seven laborious years later.

This article, in contrast to the Common Core, has only one hypothetical—a database of all the calls made and received by the clients of two major telecommunications providers and being used by an intelligence agency to detect terrorists. It only has two legal systems—the United States and Europe. Otherwise, the method is very similar.

This article is also an unconventional exercise in comparative law. It deals with a problem of public law. The field of comparative law has long been dominated—some would say "obsessed"—by the problems of contracts, torts, and property.[221] In the past, comparing constitutional and administrative law was dismissed as fruitless. Such law, unlike private law, was believed to be so unscientific and value-laden that comparison would not be able to yield any useful insights.[222] Because public law was believed to embody the distinct historical and political experience of the nation state, comparing public law could not reveal any basic truths that could serve as the grounds for universal, international regulation of different areas of human activity—traditionally the main purpose of comparative law.

Today, comparative public law is still seen as qualitatively different from comparative private law. The institutional setting in which public law operates is still believed to be more historically and culturally contingent than the sphere of civil society relations in which private law applies. As John Bell argues

---

[220] *Id.* at 17-20.

[221] Mathias Reimann, *The Progress and Failure of Comparative Law in the Second Half of the Twentieth Century*, 50 AM. J. COMP. L. 671, 680 (2002).

[222] *See generally* KONRAD ZWEIGERT & HEIN KÖTZ, INTRODUCTION TO COMPARATIVE LAW 3, 39-40 (3d ed. 1998) (on early ambition to create "common law of mankind" and continuing preference for "unpolitical" as opposed to political areas of the law).

> In public law, the core function of law is distinctive from private law. Public law is about defining and controlling the powers and activities of government. This is not the function of private law, which exists to provide frameworks within which individuals can undertake voluntarily, and to provide remedies when they exceed the bounds of the acceptable use of private power. . . Now, to talk at a very high level of abstraction, one can discuss the basic principles of liberal democratic government and the control of abuse of power. . . But if we are going to discuss the role of law, we need to descend into several layers of detail, so the question becomes: how do you govern in a liberal and democratic way in a society divided on linguistic grounds which has a relatively short history of independent government and which has a broadly French tradition of institutions (Belgium), as opposed to how do you govern a long-standing unitary state with religious divisions and with a distinct tradition of governmental institutions (Netherlands).[223]

The greater cultural and historical embeddedness of public law, however, is no longer perceived as an obstacle to comparison. Indeed, comparative constitutional and administrative law are becoming standard fare in the academy.[224] This article is part of the academic trend to remedy the earlier "obsession" with private law.

Another point of departure from the conventional method is this article's emphasis on the difference between the American and European approaches to privacy in the face of government data-mining. One classic start date for comparative law is the founding of the International Congress for Comparative Law by Edouard Lambert and Raymond Saleilles in 1900.[225] Their ambition was to find, through comparison, a common law of mankind. And, over one hundred years later, this ambition still guides the comparative work of organizations such as the United Nations Commission on International Trade Law and the International Institute for the Unification of Private Law. The cosmopolitan ideal explains, at least in part, the traditional ontological choice in favor of similarity: to see similar problems of social organization, across all legal systems, and to see similar solutions to those problems, albeit accomplished through different types of rules, styles of reasoning, legal institutions, and social practices.[226]

To be fair, this analysis of the NSA call-records program is premised on a good deal of similarity across societies. After all, the United States and Europe share a common Enlightenment heritage. Privacy is valued by both Europeans and Americans. In both places, privacy is defined as a certain degree of freedom from the scrutiny of others and a certain amount of autonomy in making life decisions. And when a

---

[223] John Bell, *Comparing Public Law*, *in* COMPARATIVE LAW IN THE 21ST CENTURY 235, 236-37 (Andrew Harding & Esin Örücü eds., 2002).
[224] *See, e.g.*, Daniel Halberstam, *Comparative Federalism and the Issue of Commandeering*, *in* THE FEDERAL VISION 213 (Kalypso Nicolaidis & Robert Howse eds., 2001); Vicki C. Jackson, *Comparative Constitutional Federalism and Transnational Judicial Discourse,* 2 INT'L J. CON. L. 91 (2004).
[225] ZWEIGERT & KÖTZ, INTRODUCTION TO COMPARATIVE LAW, *supra* note__ at 2.
[226] *See* Michaels, The Functional Method of Comparative Law, *supra* note _ at 373-74.

government acquires information about individuals, both Europeans and Americans feel that their privacy is threatened. Without privacy or a possible government harm, the hypothetical would have no meaning. The bulk of the discussion, however, is devoted to revealing how the solutions—the legal categories, the sources of law, and the outcomes—are all different.

2. The Difference: European versus American Liberty

According to the legal historian James Whitman, European privacy law protects dignity, American privacy law protects liberty.[227] In Whitman's view, the law in the two places is informed by two very different cultural values: protecting one's reputation against the vulgarities of the market and the media in Europe, protecting individual freedom from intrusions of the state, especially in one's home, in America.[228] This argument has intrigued and persuaded many privacy scholars. It explains one very puzzling difference between American and European privacy law: the apathy of American tort and constitutional law when confronted with even the grossest of privacy abuses if the offender happens to be a private actor, especially the media.[229] It also fits with the very different rhetoric of the American and European case law. In American cases, the existence of a privacy interest turns on whether an individual has a reasonable expectation of privacy, an issue that is generally addressed by examining constitutional history and social practices—all of which point to the home as the place in which individuals have been traditionally allowed to conduct their affairs free from the gaze of others. By contrast, European privacy cases, especially the German ones, begin from the need to preserve human dignity and to develop personal autonomy. In pursuing these core values, the home is always protected, but so too are spaces and personal matters outside the home.

Although this analysis has considerable merit, Whitman obscures an important aspect of European privacy law. True, European privacy law promotes inter-personal respect among individuals. But it also protects privacy against the state. And it is not always true, as Whitman argues, that "state action will raise American hackles much more than European ones."[230] Indeed, the argument of this article is that, in the context of anti-terrorism data-mining, European law protects liberty interests *more* than American law. At least European spy agencies tell their citizens when their personal data is being collected and combined and, depending on the results, sent to the police for further action, a lot more than can be said for American spy agencies.

How can this somewhat counterintuitive difference between American and European law be explained? This transatlantic difference is even more surprising in light of the specific origins of *information* privacy.

---

[227] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004).
[228] *Id.* at 116.
[229] *See, e.g.,* Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).
[230] *See* Whitman, *Two Western Cultures of Privacy*, *supra* note__at 1211.

When individual privacy in the age of information technology first became a policy problem, American policymakers were every bit as active as their European counterparts. In fact, a case can be made that European privacy law was influenced by American law and policy. The book *Privacy and Freedom*, written by the American scholar Alan Westin and published in 1967, was one of the first systematic treatments of the impact of computers on privacy. It was widely read in both the United States and Europe.[231] By the early 1970s, legislative and regulatory proposals were being floated on both sides of the Atlantic. In the United States, this was the era of the Nixon scandals. The first data-privacy proposal came from the Department of Housing, Education, and Welfare (HEW).[232] In 1973, HEW issued an influential report on government databases of personal records. To assuage public distrust of such databases, the report recommended that all government departments adhere to a Code of Fair Information Practices. Many of these fair information practices were soon after incorporated in the Privacy Act of 1974. When, in 1980, a set of data-protection guidelines were adopted by the Organization for Economic Cooperation and Development, a number of the American legal principles were included.[233] These guidelines, in turn, influenced the negotiations on the Council of Europe Convention.[234] No wonder then that the terms of the U.S Privacy Act sound awfully similar to those of the Council of Europe Convention.

Rewinding the tape again to the early 1970s, the first national data-protection laws adopted in Europe and the United States displayed remarkable similarities. This is well documented by political scientist Colin Bennett in his study of data protection in the United States, Sweden, Germany, and the United Kingdom.[235] In his study, Bennett found that the "problem" of privacy in the information technology age was similar in all four countries: it contained a humanistic dimension protecting individual dignity against the alienating aspects of mass society and information technology; a political dimension designed to prevent a tyrannical state from using information technology—and personal information—as a tool of oppression; and an instrumental dimension to advance other, non-privacy values such as equality and accuracy.[236] He also found that the national legislation was similar even though all countries, with the exception of the United Kingdom, were responding to their own internal politics and institutional concerns. The only real difference was in the regulatory styles used to advance the privacy goals—informal and negotiated in Germany and the United Kingdom, bureaucratic in Sweden, and legalistic in the United States. These early transnational similarities were reinforced by the focus, in both places, on *public sector* information abuses. Different from the U.S

---

[231] *See* Stefano Rodotà, *Information Technology—Latest Developments in Scientific Research and Regulatory Practices*, *in* ETHIK UND WISSENSCHAFT IN EUROPA 63, 66 (Dietmar Mieth ed., 2000).
[232] *See* SOLVE, ROTENBERG & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note__ at 577-83.
[233] *See* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1.
[234] *See* BENNETT & RAAB, THE GOVERNANCE OF PRIVACY, *supra* note__ at 75.
[235] *See* COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES (1992).
[236] *See* Donald F. Norris, *Book Review, Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, 87 AM. POL. SCI. REV. 1035 (1993).

Privacy Act, European laws also regulated private-sector data processing.[237] These provisions, however, were included almost as an afterthought. At the time, the principal organization with the resources, technology, and motive to process large amounts of personal data was the state.

What changed? For purposes of this article, it is not necessary to consider in depth the differences in private-sector regulation. Suffice it to say that, as the technology became more advanced, enabling a wide array of private actors to engage in data processing, the scope of European regulation expanded too. The naturalness with which the primarily public-sector framework was extended to the private sector can be put down to a number of factors: the original legislative choice to cover personal data processing, the constitutional practice—different from the American one—of applying rights to both government and private actors (horizontal effect or *drittwirkung*); and the dignity values identified by Whitman.

But why did the two systems diverge so radically in the public sector? After all, the statutes contained similar sets of legal provisions. Compared to the private sector, the changes wrought by technology to government information collection and manipulation have not been nearly as radical. In other words, the contrast cannot be put down to protecting privacy in the face of new information technology, a new policy problem that might be addressed differently by the different societies. Rather, at least three institutional forces appear to have been at work, forces not tied directly to the substance of information-privacy policy.

As already noted, one of the major differences separating American from European data-protection laws is enforcement. In the American case, the primary enforcers are individual litigants; in the European case, they are independent privacy agencies. This is consistent with broader patterns of regulation in the two legal system: Americans litigate in court and Europeans negotiate with government agencies.[238] The American choice, however, appears to have been particularly ill-suited to the realities of information privacy in the work of government agencies. The injuries suffered by individuals—not to speak of the polity—when the government secretly undertakes a program like that for call-records are generally not recognized by common law courts. When spying occurs through unobtrusive methods, without visible consequences like a criminal prosecution or civil action, it is almost impossible to prove the injury element of a tort claim. In addition, suing government is almost always more difficult than suing private parties. Even though the Privacy Act lifts sovereign immunity, the government still benefits from a form of qualified immunity: most violations of the Act must be

---

[237] A number of the congressional bills proposed in the run up to the U.S. Privacy Act would have regulated personal data processing in both the public and private sectors. Industry groups and privacy experts, however, successfully opposed such language on the grounds that it was too early to tell what kinds of privacy problems would emerge in the private sector. They also argued that the diverse circumstances of various economic sectors would be handled best in tailored sector-specific statutes, not in a cross-cutting piece of legislation.

[238] *See* ROBERT A. KAGAN, ADVERSARIAL LEGALISM: THE AMERICAN WAY OF LAW (2002); *see also* DAVID VOGEL & ROBERT A. KAGAN, THE DYNAMICS OF REGULATORY CHANGE: HOW GLOBALIZATION AFFECTS NATIONAL REGULATORY POLICIES (2004).

proven "intentional or willful" before a plaintiff can recover.[239] A government agency with the authority to investigate other agencies for privacy violations, to recommend changes if such violations are found, and, in the last resort, to impose an administrative sanction or to take an offending government official to court is likely to be a better enforcer than private attorneys general.

Administrative agencies and courts, of course, are not just enforcers but also policymakers. And as compared to generalist courts, administrative agencies have distinct advantages. Because their resources and authority are committed to specific government policies, they develop expertise, historical memory, and bureaucratic dedication in their policy areas. When political and social realities change, administrative agencies stay put; they are there to promote the goals of earlier legislative enactments. Indeed, privacy agencies in Europe would probably describe themselves as policymakers first, enforcers second. Their resources are devoted largely to vetting government proposals for proportionality and making policy recommendations in the face of new technological threats to privacy.

The lack of a similar institution in the United States is a big part of the explanation for transatlantic difference. There is no one to tell a government agency that certain personal information—say, the toll records of all AT&T customers—is not really "relevant and necessary" to accomplishing the agency's purpose.[240] Or that the agency does not review its records often enough to make sure that they are up-to-date and accurate, hence avoiding adverse consequences for individuals.[241] Or that what the agency considers to be a "routine use" of information which is "compatible with the purpose for which it was collected" really is not compatible with such purposes, thereby precluding information-sharing with another government agency.[242] Indeed, it is unnecessary to go abroad to understand the impact of the absence of a privacy agency. In most other cases in which information privacy has been regulated by Congress, an administrative agency has been charged with implementation: the Department of Health and Human Services for health privacy, the Federal Communications Commission for telemarketers, the Federal Trade Commission for children's privacy on-line.[243] In none of these areas has privacy been deemed quite as roundly and unanimously to have failed as in the case of the Privacy Act.

Another part of the explanation for the transatlantic difference, especially since September 11, is the spectacular growth of executive power in the United States. This is a trend that began in the early 1980s with the Reagan administration: first the "unitary executive,"[244] then "presidential administration,"[245] now the "wartime President." This is a well-documented phenomenon that cannot be explored in any depth here. It is

---

[239] 5 U.S.C. § 552a(g)(4).
[240] 5 U.S.C. § 552a(e)(1).
[241] 5 U.S.C. § 552a(d)(5).
[242] 5 U.S.C. §552a(a)(7).
[243] *See* SOLOVE, ROTENBERG & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note__ at 380, 666, 668.
[244] *See* CHARLES FRIED, ORDER AND LAW: ARGUING THE REAGAN REVOLUTION—A FIRSTHAND ACCOUNT 132-71 (1991).
[245] *See* Elena Kagan, *Presidential Administration*, 114 HARV. L. REV. 2245 (2001).

critical to understand the rise of executive power, however, to understand the trajectory of information privacy. The President's aggressive assertions of executive power—and the failure of Congress and the courts to react—has shaped many policy areas, including information privacy. The NSA call-records program is one, obvious illustration of this institutional logic.

Since the early 1980s, the experience of European executive branches has been quite the reverse. As the discussion of the European law illustrates, national law enforcement and spy agencies cannot simply take heed of one (national) privacy agency, one set of (national) courts. They operate in three different—in the sense of not hierarchically related—yet at the same time overlapping, legal systems: their national constitutional systems, the Council of Europe, and the European Union. The rise of Europe as a political and legal entity has been possible only by virtue of huge losses of national sovereignty. Although in some ways this might strengthen executive branches—when national ministers go to Brussels to negotiate EU laws their national parliaments cannot exercise much oversight—on the whole, the integration process has brought more and more checks on national executive power. If a Ministry of Interior wished to push back against the broad reach of European data-protection law, it would have to contend with a number of independent bodies: in the European Union, other Member States, the Court of Justice, and the Working Party of Data Protection Commissioners; in the Council of Europe, the European Court of Human Rights; and at the national level, its judicial branch and its independent privacy agency. By understanding this different configuration of executive power on the two sides of the Atlantic, we can better understand why an area of public policy that began with equal enthusiasm in both places fared so differently over time. In the United States, it met with effective opposition from the executive branch. By contrast, in Europe, once the momentum for privacy got going—and was institutionalized in the form of privacy commissioners and constitutional case law—it was very difficult for national governments to resist.

A third element that should be mentioned in seeking to explain the transatlantic difference is the European experience with the Nazis during World War II, an experience that has no American equivalent. Human rights law in Europe today, including privacy law, has been shaped by the Nazi past. This is not to say that privacy law was fashioned simply as a reaction to that experience—national legal traditions were too solidly rooted to be swept away by fifteen or so years of history.[246] But, as the historian Tony Judt puts it, for most of western Europe, World War II was an experience in profound national humiliation, a period in which the entire apparatus of state and society was put at the service of a foreign occupying power.[247] As for the Germans, at their feet lay responsibility for the atrocious human rights abuses of the Nazi regime. Throughout western Europe it was widely feared that the manipulation of the state for tyrannical ends might occur again. This fear was not abstract or irrational—it must be remembered that the Communist threat materialized even before World War II had officially come to an end. Hence all of the references to the dangers of Nazism and Communism by the

[246] *See* Whitman, *Two Western Cultures of Privacy*, *supra* note__ at 1165.
[247] TONY JUDT, POSTWAR: A HISTORY OF EUROPE SINCE 1945 14, 41(2005).

drafters of the European Convention on Human Rights.[248] And hence the German Constitutional Court's repeated references to the lessons learned from Nazism in its case law—including its privacy case law.[249] It does not seem far-fetched to conclude that European rights, including the right to stop large state bureaucracies from collecting and instrumentalizing vast quantities of information about individual citizens, have been shaped by a particularly vivid understanding of the possible abuses of state power. In the United States, after Nixon was forced to resign, Americans could forget how government power, including surveillance powers, could be used to subvert democracy and suppress rights. With the Nazis in their past and the Communists possibly in their future, forgetting was harder for Europeans.

3. Critique and Reform

By expanding the realm of legal possibilities, comparison can serve as an impetus for legal change at home.[250] Comparison brings to light the historical contingency—as opposed to cultural destiny—that informs certain legal rules and categories. By demonstrating that our national political and social aspirations have been better served by the law abroad, comparison can sharpen our sense of disappointment with our own legal experience. And looking to other liberal societies can provide a range of legal solutions—solutions that answer to the fundamental moral commitments of liberal societies but, at the same time, do not impose intolerable costs on those societies.

This exploration of European privacy law serves the agenda of legal change at home.[251] By stressing that the point of departure, in the early 1970s, was very similar on both sides of the Atlantic, the contingency of privacy law in the United States today is revealed. In my analysis of European privacy law, I have attempted to show that, indeed, that law serves principles of transparency, democratic debate, and protection against overreaching government surveillance better than American law. And, in this section, European law will serve as a point of departure for improving American law.

From the outset, two objections to this constructive comparative enterprise should be mentioned. First, some might say that even though the United States and Europe are, roughly speaking, both liberal societies, because they do not share the same moral commitments and practical constraints the privacy law of Europe cannot serve as a source of inspiration for the United States. But can it really be true that the United States is *less*

---

[248] A.H. ROBERTSON & J.G. MERRILLS, HUMAN RIGHTS IN EUROPE: A STUDY OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS 3-5 (3d ed. 1993).

[249] *See, e.g*, Bundesverfassungsgericht [BverfG] [Federal Constitutional Court], 1 Entscheidungen des Bundesverfassungsgerichts [BverfGE] (12) (F.R.G) (prohibiting neo-Nazi socialist Reich party under principles of militant democracy); 5 BVerfGE 85, 204 ff (prohibiting communist party under principles of militant democracy); 34 BVerfGE 269, 271 (Princess Soraya case); 39 BVerfGE 1, 36-37 (abortion case); 1 BvR 2378/98 of March 3, 2004, at 115 (prohibiting police bugging of homes).

[250] *See* George P. Fletcher, *Comparative Law as a Subversive Discipline*, 46 AM. J. COMP. L. 683, 695 (1998).

[251] *See, e.g.*, Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 377-80 (arguing for judicial oversight and public accountability in government data-mining and for amendments to the Privacy Act).

committed to liberty than Europe? That American citizens do not feel a need to know about government programs designed to monitor them, or to seek to confine such programs to the minimum necessary to protect them from terrorist threats? It might be, as argued earlier, that because of their different historical experiences, Americans today are less fearful than Europeans of abuses of government power: the story with which this article began—the near-escape from the conscription of Norwegian men into the Nazi army based on census records—is just that for most Americans. It is not lived history. But that good luck is not a particularly sound reason for safeguarding rights any less in the day-to-day practice of government surveillance.

Slightly more persuasive is the claim that European law has little to offer the United States because the practical constraints of the two societies are different. It is true that the United States, unlike Europe, is the world's military hegemon. In threatening, or actually conducting, military operations abroad, the intelligence needs of the United States are extensive. Moreover, because of such military operations, the United States might be more vulnerable to terrorist attacks at home, on American soil. Ultimately, however, such objections to comparison are unconvincing. It is difficult to understand the connection between unfettered data collection and data-mining at home and military operations abroad. Not only is information-gathering on individuals in the United States less likely than traditional military surveillance to garner intelligence on, say, al Qaeda's operations along the Pakistan-Afghanistan border but the constraints placed by European law on personal data processing related to military operations abroad are mild, indeed. As for the threat of terrorist attacks on national territory, the United States might be a better symbolic target, but logistically speaking it is probably easier to organize and carry out such attacks in Europe. That difference has nothing to do with civil rights law and everything to do with the size and cohesiveness of European immigrant populations and Europe's proximity to the Middle East.

A second objection to my constructive ambition is known in the comparative law literature as the "transplant problem." Like the functionalist method, drawing on the results of comparison to make suggestions for law reform is a conventional use of comparative law.[252] But, according to the post-modern critique of the past decade or so, it is also a dangerous use of comparative law.[253] The critics point to the substantial barriers to cross-cultural communication. Different societies are constituted by radically different systems of meaning that are inaccessible to most outsiders, certainly to casual academic tourists such as comparative lawyers. This, of course, is a caricature of the post-modern view. It highlights, however, one of the important insights of the post-modern critique: the cultural distinctiveness and internal coherence of any system of legal rules, modes of reasoning, institutions, and social practices.

This radical pluralism complicates enormously the task of the comparative lawyer.[254] It casts doubt on the ability of comparative law to identify any one area of

---

[252] *See, e.g.*, ESIN ÖRÜCÜ, THE ENIGMA OF A COMPARATIVE LAW: VARIATIONS ON A THEME FOR THE TWENTY-FIRST CENTURY 37 (2004).
[253] *See* Reimann, *The Progress and Failure of Comparative Law*, *supra* note__ at 680.
[254] *See* Palmer, *From Lerotholi to Lando*, *supra* note__ at 5-6.

social life to study across legal systems—to identify the functionalist "problem." Assuming a researcher is able to narrow the field of inquiry, once she goes abroad, it is highly likely that she will misinterpret the foreign law, arriving at wrong conclusions as to the meaning and consequences of the law in that society. And, in the unlikely event that she is able to surmount all of those barriers, she will never be able to bring the foreign law back home. Even if foreign law appears to work better, it will never have the same effect in the different social and cultural terrain of home.

This last piece of the post-modern critique is known as the transplant problem. And, in some regards, that is what I am proposing to do with the European law of privacy. It appears, however, that caution rather than paralysis is the best lesson to take away from the disciplinary debates of comparative law. The European privacy solution has a number of different components: a fundamental right to information privacy and a statutory scheme regulating personal data processing in the public and private sectors. The suggestion is that Americans borrow only from the statutory scheme, and only from that part curbing the government's use of personal information. In essence, the suggestion is not to transplant at all, but to reinforce the U.S. Privacy Act and, in doing so, to return to the original intent of 1974.

At the present time, an American constitutional right to information privacy is not worthwhile pursuing. Such a constitutional right would trigger judicial review of government data-mining programs similar to the European proportionality inquiry, under the guise of substantive due process.[255] Partly, this solution is unattractive because it is implausible: it is extremely difficult to imagine the current Supreme Court expanding so dramatically the constitutional right to privacy.

Pressing for a constitutional right to information privacy, however, might be unwise also for reasons of the broader institutional context.[256] In Europe, the relationship between constitutional courts and legislatures tends to be symbiotic.[257] It is not necessary to look far for examples of this relationship. The decision of the German constitutional court proclaiming a right of "informational self-determination" prompted a slew of federal and state laws to come into compliance with the constitutional standards set down in that decision.[258] Among these was an amended Federal Data Protection Act, with the declaration, in the very first line, that the purpose of the Act was to "protect the individual against his right to privacy being impaired through the handling of his personal data."[259] A number of additional changes were made to the Act, to further the new, constitutionally mandated criteria for lawful personal data processing. In the European

---

[255] *See* KOMMERS, THE CONSTITUTIONAL JURISPRUDENCE OF THE FEDERAL REPUBLIC OF GERMANY, *supra* note__at 46 (on the equivalence between German proportionality and American fundamental rights doctrine).

[256] In this respect, the law reform proposed in this article is more modest than what has been advocated elsewhere. Paul Schwartz, *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*, 37 AM. J. COMP. L. 675 (1989).

[257] *See, e.g.*, KOMMERS, THE CONSTITUTIONAL JURISPRUDENCE OF THE FEDERAL REPUBLIC OF GERMANY, *supra* note__ at 53-54.

[258] *See* Schwartz, *The Computer in German and American Constitutional Law*, *supra* note__, at 698-99.

[259] Federal Data Protection Act § 1.

Union, too, this mutually reinforcing relationship exists: the case law of the European Court of Justice is often incorporated, word-for-word, in subsequent legislation and serves as a springboard for positive legislative measures in favor of basic rights.[260]

In the United States, according to a number of prominent accounts, this relationship is quite different: when the Supreme Court takes action, Congress does nothing.[261] And vice versa, when the Supreme Court fails to act, Congress steps in with legislation. Thus, when the Court refused to protect bank records under the Fourth Amendment, Congress enacted the Right to Financial Privacy Act.[262] When the Court denied Fourth Amendment protection to pen-register information, Congress enacted the Pen Register Act. In other words, the risk is that if the Supreme Court finds a right to information privacy, Congress will not regulate government data-mining. Indeed, Congress might test the limits of the right to information privacy by authorizing intrusive federal programs that might—or might not—be struck down by the Supreme Court. Yet in this technologically complex area, a fine-tuned regulatory scheme is more essential to protecting the right than the rather blunt device of judicial review.[263] In addition, at least to begin with, legislative reform is a more legitimate mode of accomplishing change than judge-made law.[264] The opportunities for democratic participation in the legislative process are more extensive. Legislation can be more easily revised over time: notwithstanding the difficulties of repealing a law, they pale in comparison with reversing a Supreme Court precedent. The legislative branch, therefore, appears to be the venue best-suited to a privacy reform agenda.

Nor would it be necessary for Americans to adopt a comprehensive data-protection law, covering all data processing in both the private and public sectors. Without a doubt, European limitations on personal data processing in the market make government programs like the NSA call database vastly more difficult. This aspect of European data-protection law also affords greater visibility and accountability to any such government initiative: there must be a law or regulation authorizing the government to request personal data *and* permitting private firms to keep personal data. However, a comprehensive U.S. data-protection law would require a radical change of the legal environment: market actors would be asked to limit their data processing operations across-the-board, not just in a few specific areas like health care, telecommunications,

---

[260] *See, e.g.*, Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 (on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast)), 2006 O.J. (L 204) 23 (sex equality in the workplace); GEORGE A. BERMANN ET AL., CASES AND MATERIALS ON EUROPEAN UNION LAW 511 (2d ed. 2002) (free movement of goods).

[261] The logic behind this congressional inaction varies. *See* William Stuntz, *The Political Constitution of Criminal Justice*, 119 HARV. L. REV. 780, 797-98 (2006) (political incentives); Erwin Chermerinsky, *The Religious Freedom Restoration Act is a Constitutional Expansion of Rights*, 39 WM. & MARY L. REV. 601 (1998) (Supreme Court's separation of powers doctrine).

[262] *See* SOLOVE, ROTENBERG & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note__725, 271.

[263] *See generally* STEPHEN BREYER ET AL., ADMINISTRATIVE LAW AND REGULATORY POLICY: PROBLEMS, TEXT, AND CASES 16-35 (5th ed. 2002) (describing evolution of administrative state from common law courts to specialized regulatory agencies).

[264] *See* ALEXANDER M. BICKEL, THE LEAST DANGEROUS BRANCH: THE SUPREME COURT AT THE BAR OF POLITICS 16-23 (Yale Univ. Press 1986) (1962) (describing countermajoritarian difficulty).

and financial services as under the current system. Such a change, moreover, might not be particularly well suited to a common law legal system. A wide range of firm activities that are currently subject to the tort and contract law of common law courts would be swept into a statutory scheme, subject to the different mode of deciding and enforcing duties entailed by such a scheme.[265] And all of this upheaval would produce relatively little benefit for the problem at hand: it would not directly curb data-mining by *the government*.

Coming to the recommended reform: A few changes to the U.S. Privacy Act would advance the cause of information privacy enormously. The ambition should be to close some of the gaps that have allowed for the divergence, over time, of the American and European systems. Many of these gaps, indeed, were not anticipated by the drafters of the Privacy Act but were produced by weak judicial enforcement combined with aggressive bureaucratic interpretation. First, it should be made absolutely clear that the Privacy Act catches all government programs that involve large-scale personal data processing. The kind of Orwellian, Big-Brother abuses against which the Privacy Act was directed are just as likely with anti-terrorism data-mining as with systems designed to retrieve information on welfare recipients for purposes of determining their benefits. This broader coverage might be achieved by re-writing the statute to include a new definition of the statutory term "system of records" or substituting that term with a new one. This change could also be accomplished by the judicial branch. The legal uncertainty concerning the scope of the Privacy Act—and whether it covers data-mining programs like the NSA call database—is largely a product of the inconsistent case law of the federal courts.[266] This shortcoming, therefore, could very well be fixed by those same courts.

Second, the Privacy Act's exemptions for intelligence and law enforcement agencies and their activities should be narrowed considerably. These are the government bodies and public programs that are most dangerous to individual liberty. The potential for government abuse of private information is greatest when such information is collected by the police—or handed over to the police by government spies. No other organ of the state has the power to do as much harm to individual citizens. The very reason for these powers, of course, is the critical public-safety mission with which the police are entrusted. Yet the carefully constructed German and French exceptions for police forces and security agencies demonstrate that it is possible to strike a more reasonable compromise between individual privacy and public safety. The German and French examples demonstrate that it is *not* necessary to allow such agencies to go entirely unregulated.

Third, the exception in the Privacy Act for "routine uses" of personal data should be repealed. This exception has enabled federal agencies to share personal information

---

[265] *See generally* JOHN HENRY MERRYMAN, THE CIVIL LAW TRADITION (2d ed. 1985) (comparing precedent-based common law tradition and code-based civil law tradition); GUIDO CALABRESI, A COMMON LAW FOR THE AGE OF STATUTES (1982) (comparing common law decisionmaking and statutory interpretation).

[266] *See supra* note__ and accompanying text.

with other federal agencies, as well as state and local bodies, virtually unchecked. If the routine use exception is not repealed, then much of the benefit gained from covering national security and law enforcement agencies will be lost: the restrictions on sharing private data with law enforcement agencies at the federal and state level would be laughable. Free-for-all information sharing is precisely what has been condemned by the German constitutional court.[267] In the United States, it is also cause for concern in the more traditional area of wiretapping: the so-called FBI "wall" between law enforcement and intelligence officers was established to prevent criminal prosecutors from using national security surveillance to obtain information on all offenses, regardless of their seriousness.[268] The danger of using the far-reaching powers of spy agencies to investigate mundane crimes like tax evasion—for legitimate public or illegitimate political reasons—is as present when personal data is collected and analyzed. Someone's phone records, combined with information on their bank transfers, can be as revealing to the police as their actual conversations. Whenever authorizing a new government program, therefore, agencies should be required to specify, up front, exactly how personal data will be used and under what conditions it will be transferred to other government agencies.

Last, the enforcement scheme in the Privacy Act should be amended to include an independent privacy agency. An independent privacy agency would offer a solution to some of the most serious deficits of the Privacy Act. This recommendation, of course, is inspired by the European institution but it also has a solid domestic foundation. The original bill contained such an agency, but it was removed in the end as part of the compromise necessary to pass the Privacy Act. A later bill, proposed in 1991, would have established a Data Protection Board, with powers similar to those of European privacy agencies. The bill passed in the House of Representatives but never made it through the Senate.[269] In fact, many European privacy agencies are modelled after the independent agencies of the U.S. administrative state.[270]

The consequences of the absence of an administrative agency have already been explored here in explaining the divergent paths of privacy law in the United States and Europe. For the present purposes of reform, however, the deficiencies of the current system should be reviewed with some more precision. Under the Privacy Act, individuals have a right of action for injunctive relief and damages against the government.[271] This remedy, however, is inadequate for a number of reasons. Injunctive relief is available for only two types of violations of the Privacy Act: the government refuses an individual access to her personal records or refuses to correct her personal records. Damages may be awarded for any other violation of the Privacy Act that has an "adverse effect" on an individual. The circumstances under which recovery is

---

[267] *See* Judgment on G10 Amendments, *supra* note__.
[268] *See* SOLOVE, ROTENBERG & SCHWARTZ, INFORMATION PRIVACY LAW, *supra* note__ at 39.
[269] *See* H.R. 685th To establish a Data Protection Board, and for other purposes, 102d Congress 1st Session, Jan. 29, 1991, *reproduced in* WAYNE MADSEN, HANDBOOK OF PERSONAL DATA PROTECTION 887-92 (1992).
[270] *See generally* GIORGIO GIRAUDI & MARIA RIGHETTINI, LE AUTORITÀ AMMINISTRATIVE INDIPENDENTI (2001) (describing influence of U.S. model on Italian and French independent agencies).
[271] 5 U.S.C. § 552a(g).

permitted, however, are limited. Plaintiffs must prove a "willful or intentional" violation of the Act. Plaintiffs must show actual damages—and emotional damages alone generally do not count—before they can qualify for the Privacy Act's minimum damages award of $1,000.[272] The real problem for enforcement, however, is that many privacy violations go undetected or do not result in injury traditionally recognized by the courts. If there were restrictions on transferring personal data between intelligence and law enforcement agencies, and these were breached, it is unlikely that an individual would ever learn of the breach. If she did, she would be able to show damages only in the extreme circumstances of intrusive surveillance or an arbitrary detention. Because of this mismatch between data-privacy injuries and the common law's remedial architecture, an independent body with oversight and enforcement powers is essential.

An independent privacy agency would also foster greater transparency, public debate, and, yes, privacy, at the drawing-board phase, at the time that new government initiatives are designed. Under the Privacy Act, government agencies are already required to publish Privacy Notices in the Federal Register when they plan on creating or modifying a system of records.[273] A privacy notice must contain information on the type of personal data in the system, the purposes for which the data will be used, the security measures in place to protect the data, the other agencies with which the personal data will be shared, and the procedures available to individuals to access and correct their records.[274] The notice requirements could very well be expanded to include the steps that had been taken by the agency to ensure the necessity, relevance, and adequacy of the personal data, as well as to consider less privacy-intrusive alternatives to the proposed system of records. With the fewer exceptions envisioned above, agencies would be required to provide this detailed explanation for a wider range of activities. An independent privacy agency would be in a position to provide an expert, impartial analysis of the privacy implications of the proposed program. Furthermore, in areas of government activity such as national security—in which disclosure can sometimes defeat the purposes of the government program—scrutiny by an independent agency would serve as a proxy for public debate. In other words, if secrecy is absolutely necessary, an independent privacy body would bring an important outsider perspective to an area of government activity that, by definition, cannot draw on the valuable insights of broad-ranging public scrutiny.

CONCLUSION

With the exception of an independent privacy agency, these proposed legal changes are modest. They draw on the European experience yet they are thoroughly

---

[272] *See* Doe v. Chao, 540 U.S. 614 (2004).

[273] 5 U.S.C. 552a(e)(4). The government must also conduct a privacy impact assessment before establishing a new program involving personal data. E-Government Act § 208, 44 U.S.C. § 3501 (note). The information, however, contained in impact assessments is very similar to that in privacy notices. Furthermore, impact assessments are not required for national security systems. E-Government Act § 202(i), 44 U.S.C. § 3501 (note).

[274] *See, e.g.*, Transportation Security Agency, Notice to Establish System of Records (Secure Flight Test Records), 69 Fed. Reg. 57,345 (Sept. 24, 2004).

grounded in the text of the original Privacy Act. Even the creation of a independent privacy agency, part of the original legislative package that became the Privacy Act, is consistent with past and current trends in American law. Since September 11, a number of special-purpose privacy watchdogs have been created by Congress to address civil liberty concerns: the Chief Privacy Office in the Department of Homeland Security,[275] the Privacy and Civil Liberties Board in the Executive Office of the President,[276] and the Civil Liberties Protection Officer in the Office of the National Intelligence Director.[277] These civil liberties aims would be better achieved through a single privacy watchdog, with powers extending to the entire federal administration and with independence from the government officers in charge of privacy-burdening programs.

These improvements, in fact, would lead not only to better protection of privacy, but also to a more effective government response to the national security threat. In European eyes, such changes would constitute a satisfactory guarantee that the privacy of European personal information will be protected once transferred to American authorities. This would facilitate tremendously the transatlantic exchange of intelligence among government authorities. Thus the borderless realm of twenty-first century terrorism would be matched by public action also capable of overcoming the confines of the nineteenth-century nation state.

---

[275] 6 U.S.C. § 142. For a comprehensive analysis of these privacy watchdogs see Marc Rotenberg, The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight after 9-11 (paper on file with author).
[276] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458 § 1061 (2004).
[277] *Id.* § 1097 (codified at 50 U.S.C. § 403-3d).