2015

The Pond Betwixt: Differences in the U.S.-EU Data Protection/Safe Harbor Negotiation

Richard J. Peltz-Steele
University of Massachusetts School of Law - Dartmouth, rpeltzsteele@umassd.edu

JOURNAL OF INTERNET LAW
VOLUME 19
NUMBER 1
JULY 2015
EDITED BY DLA PIPER

The Pond Betwixt: Differences in the US-EU Data Protection/Safe Harbor Negotiation

By Richard J. Peltz-Steele

Since the adoption of the 1995 Data Protection Directive (Directive)[1] in the European Union, data sharing between Europe and the United States has been problematic. The Directive made concrete in law and policy a conception of privacy that had been diverging from its US counterpart for decades. Nevertheless, in the first decade of the 21st Century, a "safe harbor" and related agreements (together, Safe Harbor)[2] stitched together a peace. Though at times the peace rested uneasily, it bridged the Atlantic sufficiently to allow commerce and innovation in technology and information to flourish largely unhindered by restrictions on international data transfers.

But in the 2010s, the gulf between the continents has widened, and the bridge is stressed to a possible breaking point. The Snowden revelations of US government surveillance have exacerbated tensions. Meanwhile ambitious efforts to overhaul the Directive for the new era of interconnected electronics and invasive technology has proven contentious both within Europe and abroad. Transnational business now watches intently as behemoth political powers struggle to refashion world privacy policy with far-reaching implications for human rights and economic liberty around the world.

This article analyzes the differing perspectives that animate US and EU conceptions of privacy in the context of data protection. It begins by briefly reviewing the two continental approaches to data protection and then explains how the two approaches arise in a context of disparate cultural traditions with respect to the role of law in society. In light of those disparities,

Continued on page 15

Richard J. Peltz-Steele *is a professor at the University of Massachusetts Law School in Dartmouth, MA.*

Wolters Kluwer

The Pond Betwixt
from page 1

the final discussion focuses on points of disparity that are unlikely to be overcome in short-term negotiations and advises each side on moving forward.

TWO VANTAGES

International politics and economics being what they are, privacy law and policy in the United States and Europe reverberate throughout the world. To be sure, US and European conceptions of privacy emerge in a Western legal tradition that is far from universal. Viewed from a truly global cultural perspective, the trans-Atlantic divergence is not so broad. But US and EU approaches today vie not only for north Atlantic dominance, but as models for the world. So the study of this divergence, and how it emerged from a shared cultural heritage, merits scrutiny.

COMMON FONT

Underpinning contemporary data protection regulation is the normative value that both US and EU societies place on personal privacy. Both cultures attribute modern privacy to the famous Warren-Brandeis article in 1890, outlining a "right to be let alone."[3] But decades passed before the impact of the article was felt. Notwithstanding the dramatic achievement of women's suffrage, human rights in the early 20th Century were marred by the two World Wars and failure of the League of Nations. After World War II, privacy came into its own. The word appeared explicitly in Article 12 of the Universal Declaration of Human Rights,[4] adopted by the General Assembly in 1948. With the drafting in 1950 of the European Convention on Human Rights (ECHR),[5] however, the United States and Europe committed to divergent paths.

PRIVACY AND DATA PROTECTION IN EUROPE

Both privacy and data protection are today part of the fundamental rights system of Europe, a component of the amalgamated constitution of the European Union. Both are part of the legislative and regulatory state at the national and federal levels. This remarkable ubiquity of privacy and data protection in European law has come into being substantially in just the last half century.

Constitutional Law

Privacy is safeguarded by ECHR Article 8, modeled in its 1950 original after the 1948 Universal Declaration. The right appears in the dichotomous expression typical of modern human rights guarantees, one provision broadly articulating the right, followed by a second provision that authorizes public limitation when "necessary in a democratic society." Whereas the Fourth Amendment in the United States is a negative assertion designed to curtail state power from infringement of individual liberty—referencing a right that "shall not be violated"—the European right of privacy is a positive declaration.

By the 1970s, the ECHR was showing its age. To meet the challenges of the nascent information age, the Council of Europe in 1980 adopted the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data,[6] known as "Convention 108" after its catalog number in the European Treaty Series. Convention 108 introduced the notion of balance in the data protection context, "[r]ecognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples."[7] The convention furthermore singled out "privacy" as a "particular" motivation among its human-rights aims,[8] and the term appears three times in the convention's substantive provisions.[9]

The right to privacy was folded into Article 7 of the 2000 Charter of Fundamental Rights of the European Union, (Charter)[10] made binding on the European Union through the 2007 Treaty of Lisbon,[11] effective 2009. The Charter does not expressly limit rights by public necessity in the old dichotomous style, but incorporates permissible limitations in national law by reference to the source rights and responsibilities as articulated in the ECHR.[12]

Critically, the Charter in its Article 8 "recognize[d] the right to the protection of personal data as a new fundamental right, distinct from the [article 7] right to respect for private and family life, home and communications."[13] Accordingly the European Commission regards data protection as a member of the "third generation" of fundamental rights alongside governmental transparency and "bioethics guarantees," the latter also privacy inspired.[14]

Article 8 has three provisions. The first broadly proclaims "the right to the protection of personal data." The second provision concerns data processing. First it requires that "data … be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law." Second it proclaims a right of access to data and a right to rectification of error. The third provision requires that data protection compliance be controlled by "an independent authority," that is, by an entity at arm's length from the conventional machinery of each national government.

Law and Regulation

Those particular data protection concepts enshrined in the 2000 Charter—limited and consensual processing, access and rectification, and supervisory independence—were by then known principles of the European data protection regime—established by the 1995 Directive.[15]

The Directive has been well summarized in the literature.[16] It is broad in scope. The "personal data" that triggers regulation is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly," even by a reference number or descriptive characteristic.[17] Data "processing" is "any operation or set of operations which is performed upon personal data," including collection, transmission, and destruction.[18] Regulated data "controllers" and "processors" include any persons or entities responsible for data processing, public or private.[19]

Any data processing must be "legitimate," and legitimacy is dictated by disjunctive criteria, which include subject consent, legal obligation, vital interests of the subject, public interest, and "legitimate interests" not contravened by fundamental rights.[20] In broad strokes, the Directive articulated a series of fair information practices (FIPs) that have become well recognized norms, namely:

- **"data minimization,"**[21] meaning that data controllers should collect and retain data only as befits the purpose of its use;[22]
- **notice, access,** and **correction**: all provisions in the later vein of Charter article 8(2), regarding the obligation of data controllers to inform data subjects about the collection and processing of their data, affording opportunity for access to that data and correction, or rectification, of errors;[23]
- **transparency** of data processing,[24] especially with regard to the logic behind automated data processing, a safeguard that means in part to forestall *de facto* discrimination resulting from the use of analytics;[25]
- **consent** of data subjects to the processing of their data, "freely given[,] specific[,] and informed";[26]
- **"sensitive data"**[27] classifications, such as medical and financial, and that trigger a higher level of protection;[28]
- **security**, to protect data against misuse, loss, and theft;[29]
- **enforcement** of data protection law through national supervisory bodies;[30] and
- **independence** of the national supervisory bodies.[31]

As a "directive" in European law, the data protection law must be implemented at the national level. As a piece of federal legislation, the Directive is subject to definitive interpretation by the European Court of Justice. Furthermore, the Directive in its article 29 constitutes a "Working Party," comprising national data protection supervisors and representatives of European Community bodies and of the European Commission.

The Directive contains a number of important limitations. Data processing limitations pertain only within the scope of European Community law, though data transfers onward to third countries are permissible only if "adequate" data safeguards are in place on the receiving end.[32] The Directive exempts from its scope state data processing for purposes of national security and criminal law enforcement.[33] "[A] natural person in the course of a purely personal or household activity" also is exempt.[34]

Proposed Regulation

Now 20 years old, the Directive is dated. The Internet was far from ubiquitous in 1995, and mass data processing was the occupation of a manageable range of public and private actors. Technological advancements have brought daily life within the ambit of the Directive, and globalization in commerce has tested the reach of the Directive. Meanwhile the passage of time has resulted in increasing variegation in the interpretation, application, and enforcement of

data protection across Europe. The sum of these pressures was a movement in the European Parliament to overhaul and supersede the Directive with a new General Data Protection Regulation (Proposed Regulation).

The European Commission published a draft text for the Proposed Regulation in January 2012.[35] The ambitious project has spurred quarrels within Europe—even a competing draft from the European Parliament[36]—and drawn fire from abroad, namely media and business interests in the United States. At the time of this writing in spring 2015, adoption seems more likely in 2016 than in 2015, with an effective date two or three years later.

The Proposed Regulation also has been explicated in the literature.[37] As a regulation rather than a directive, it will be a self-executing law among EU member states, not contingent on the enactment of domestic legislation. In short, the Proposed Regulation will beef up fair information practices. Consent standards are more demanding, transparency requirements are more explicit, and liability and sanctions for noncompliance are more severe. Supervision and enforcement are toughened, and consistency enhanced, with the creation of a European Data Protection Board, composed of national data protection supervisors.

Critically, the Proposed Regulation extends its territorial reach outside the European Community, to any entity within the reach of EU jurisdiction that "offers goods or services to … data subjects in the Union" or "monitors their behavior."[38] The Proposed Regulation thus sweeps in the lot of multinational companies that do business with EU citizens, regardless of a company's geographic location. That expansion is what has drawn the attention, and in some cases the ire, of US interests.

PRIVACY AND DATA PROTECTION IN THE UNITED STATES

It comes as a surprise to the casual observer of US law that there is in the United States any kind of systematic protection for data privacy. Indeed, "systematic" is a generous word. But Warren-Brandeis privacy did originate in the United States, and the Internet era has seen a burgeoning complex of law and regulation in privacy, however much lacking in unifying strategy.

Constitutional Law

The lack of explicit mention of privacy in the US Bill of Rights has slowed but not stopped the development of privacy as a constitutional concept. But two features of US constitutional design—federalism and negative civil rights—have important implications for how privacy is and may be developed in US law.

First, the US Constitution created a rigid federal structure, bolstered by the Tenth Amendment and limited by the Reconstruction Amendments. The observance of vertical separation of powers has been a hallmark of the conservative political platform and conservative constitutional jurisprudence since the civil rights era—witness the debate over universal healthcare in federal law. As a result, the federal government must navigate the complexities of its limited powers to erect a nationwide level floor of statutory and regulatory privacy protection.

Second, the Bill of Rights, as incorporated through the Fourteenth Amendment, is a negative legal instrument, designed to shield people against the power of government.[39] As a result, US constitutional privacy law is powerfully influenced by the state action doctrine. Constitutional manifestations of privacy in the United States are not well equipped to frame a modern system of data protection that tackles challenges in the public and private sectors alike.

At least when state action is implicated, privacy has manifested as a constitutional value in three dimensions: (1) the right to personal autonomy, (2) the right to be let alone, and (3) the right to informational privacy.

The first vein of constitutional privacy, personal autonomy, comes closest to the broad European conception of privacy as a basic dignitary interest. This is the right of privacy that operates in the abortion cases, in essence affording a woman pre-viability access to abortion services subject to state constraints that do not unduly burden the right.[40] Consequently, autonomy-privacy has been swept up in the vitriol of the abortion controversy. The bitter political, social, and jurisprudential divides cast a long shadow over every discussion of privacy as a constitutional concept. Autonomy-privacy is not so limited, though, and has a broad range of potential application, especially in medical decisionmaking. Autonomy-privacy has been at stake in the US Supreme Court's "right to die" cases, one finding a constitutional right to

refuse unwanted treatment,[41] and another rejecting a constitutional right to assisted suicide.[42]

The second vein of constitutional privacy, the right to be let alone, or to seclusion, traces its lineage directly to the 1791 Bill of Rights. In Fourth Amendment jurisprudence, the controlling concept in defining the scope of the right against unreasonable searches and seizures has been the "reasonable expectation of privacy."[43] This test is criticized today as incompatible with a fundamental, so undiminishable, right.[44] Reasonable expectation, a floating norm, necessarily diminishes in the panopticon of the online world.[45] Making matters worse, the reasonable expectation of privacy is limited dramatically by the third-party doctrine, which holds that privacy is forfeit when information is voluntarily submitted to a third party, such as a bank or communication service provider.[46] This stark division between information secret because it is secreted, and information not secret because it is disclosed—termed "the secrecy paradigm" by Professor Daniel Solove[47]—persists as a norm in US privacy law. But what might at one time have accorded with a societal sense of reasonableness no longer does—as evidenced by popular objection to the dragnet collection of communication metadata by the US intelligence service.

The third vein of constitutional privacy, the right to informational privacy, has been assumed *arguendo* by the US Supreme Court on three occasions, but remains a largely uncharted sea. In all three cases, the Court concluded that public access to personal information was sufficiently justified or constrained to surmount the objections of data subjects. In *Whalen v. Roe*,[48] the Court rejected a challenge, based on informational privacy and autonomy-privacy, to a New York criminal enforcement system that monitored drug prescriptions. In *Nixon v. Administrator of General Services*,[49] the Court determined that the statutory-regulatory framework for reviewing and preserving executive records adequately protected the informational privacy interests of former President Nixon. More recently, in *NASA v. Nelson*,[50] the Court rejected a constitutional challenge to security background checks on space-agency contractors.

Statute and Common Law

While lacking a comprehensive privacy law, the US Congress has enacted a number of sector-specific privacy laws, usually using the Commerce Clause[51] as the source of federal legislative authority. These statutes include the Fair Credit Reporting Act (FCRA) (1970),[52] the Family Educational Rights and Privacy Act (FERPA) (1974),[53] the federal Privacy Act (1974),[54] the Video Privacy Protection Act (VPPA) (1988),[55] the Health Insurance Portability and Accountability Act (HIPAA) (1996),[56] and the Children's Online Privacy Protection Act (COPPA) (1998).[57]

Each law defines its own scope in accordance with the problem it anticipates, and each its oversight or enforcement mechanism, invariably public rather than private. For example, FERPA governs public and private educational institutions receiving public funds (virtually all of them) with respect to student data, and HIPAA governs defined healthcare providers with respect to patient data. FERPA is enforced by the Department of Education[58] with regulated entities' funding in jeopardy (though no de-funding has ever occurred).[59] HIPAA is enforced by the Department of Health and Human Services[60] and threatens heavy civil fines as well as criminal jeopardy.[61] Neither authorizes private enforcement.

More recently, strident legal means of data protection have emerged in three more venues: (1) data breach notification laws, (2) consumer protection law, and (3) common law tort. Forty-seven states, Washington, DC, and three territories now have data breach notification laws.[62] They vary widely in their particulars; 14 states, Washington, DC, Puerto Rico, and the US Virgin Islands authorize a private cause of action.[63] A key law exists too at the federal level, limited to the finance sector: the Gramm-Leach-Bliley Act, formally known as the Financial Services Modernization Act of 1999.[64] As hacking and data breaches continue to make headlines, the adoption of a cross-sector federal law seems inevitable.[65]

Second, data protection has emerged in consumer protection law. Born with the US regulatory state in the early 20th Century, the Federal Trade Commission (FTC) has characteristically broad authority under Section 5 of the FTC Act to regulate "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[66] Accordingly, the FTC has deployed its authority in furtherance of the simple proposition that a company must do what it says it does. So if a company says that it maintains data security, that statement becomes a promise to the consumer, enforceable by the FTC. The scope of

that enforcement authority is now being tested in the Third Circuit.[67] Target of an FTC enforcement suit, Wyndham Worldwide Corp., a global hotelier, is arguing that the FTC lacks statutory authority to bind commercial entities to reasonable data security standards.[68]

A third and very recent avenue of data protection is now emerging in common law tort. Despite the lack of a private cause of action in sector-specific privacy statutes, some victims of data security breaches have found traction in common law negligence, predicated on the violation of privacy law.[69] A negligence *per se* theory fits well with HIPAA-designed classes of plaintiff, hazard, and harm, and the Connecticut Supreme Court found HIPAA not preemptive.[70]

Proposed Consumer Privacy Bill of Rights Act

In late February 2015, the White House published a discussion draft of a bill, the Consumer Privacy Bill of Rights Act (CPBRA).[71] The draft drew together ideas that had been fomenting for some time. Consumer bills of rights already have been floated on Capitol Hill, and the White House language closely tracks ideas published two years earlier in an executive white paper.[72] Politics being what it is in Washington in the last two years of the Obama Administration, the CPBRA probably will not get traction in this Congress. But with keen bipartisan interest in consumer protection, and even the support of industry seeking to reduce costs through harmonization in domestic and international regulatory compliance, the CPBRA might prove influential in the eventual development of cross-sector privacy legislation in the United States.

The CPBRA would maintain federal focus on consumer privacy in commercial transactions, so the law is not cross-sectoral in every respect. The hook for federal jurisdiction is the Commerce Clause.[73] Enforcement authority remains with the FTC and exclusively public,[74] though state attorneys general are authorized to bring enforcement actions in the absence of FTC action.[75] Protected information relates to consumer identity, including names, financial account identifiers, and communication identifiers, such as an online user's Internet Protocol address.[76] The CPBRA broadly defines "covered entities" by excluding governments, individuals acting non-commercially, and small businesses—data processing from fewer than 10,000 individuals or devices per 12 months, or employing fewer than six persons, except where sensitive data are concerned.[77] Substantial civil penalties attend violation of data protection standards, up to $35,000 per day, or $5,000 per consumer, to a maximum of $25 million.[78]

The CPBRA drives its FIPs with 11 "context" factors, including the scope of the regulated entity's interaction with the data subject, the nature of the regulated entity's business in goods or services, foreseeability and customary business practices, the age and sophistication of the data subject, and security measures employed by the regulated entity.[79] The FIPs themselves include:

- **data minimization** in collection, retention, and use;[80]
- **notice** requirements;[81]
- **reasonable control** over data in proportion to the risks in event of compromise;[82]
- **reasonable use** of data in light of context;[83]
- **revocable consent**;[84]
- **reasonable access, correction or destruction,** and **accuracy**;[85]
- **deletion, destruction, or de-identification** of data upon expiry of the processor's purpose;[86] and
- **reasonable security** and **accountability** measures to protect data.[87]

Data processing that is "not reasonable" still may be permitted if a regulated entity conducts an appropriate privacy risk analysis,[88] and a regulated entity may apply to the FTC for pre-approval of a code of practice as a safe harbor.[89]

The correction and accuracy provisions exempt information obtained from government sources, so providing a sort of fair-reporting privilege.[90] Also the CPBRA defers repeatedly—in a global provision and in specific limitations on duties—to the First Amendment rights of regulated entities.[91] That latter qualification might cut deeply into the obligations the law would impose, insofar as a commercial entity has a First Amendment right to republish lawfully obtained truthful information.[92]

Reaction to the White House draft was swift and critical from both sides (perhaps a good sign). A representative of a consumer-protection organization declared the bill too "full of loopholes" to afford consumers "meaningful control of their data."[93] Rep. Ed Markey (D-MA) called for a statutory reform offering

"uniform and legally enforceable rules" rather than flexible factors.[94] At the same time, an advocate for the advertising industry criticized the draft bill as "an attempt to prevent theoretical harms," "sure to put a deep chill" on information innovation.[95]

THE POND BETWIXT

TECTONIC DIFFERENTIAL

Obviously substantial differences separate EU and US privacy law.[96] The former is comprehensive, the latter sectoral. Differences derive from a disparity between each continent's foundational thinking about law and society, especially with respect to civil rights. And the differences play out in each continent's capacity and willingness to legislate in privacy and data protection.[97]

Europe embraces a social-democratic form of government. Fundamental rights are dynamic and evolving. Government has an affirmative duty to the public to foster this evolution through the positive operation of law, bolstering and expanding individual autonomy. Law advances policy choices that are distributive, or allocative, of societal resources, in accordance with the normative choices of democratic bodies. Individuals owe a duty to one another in an interdependent system of social responsibility.

The United States embraces a libertarian model of government. Fundamental rights derive from a relatively static Constitution. Rights may be adapted through interpretive jurisprudence, if not through strict originalism and textual amendment, but living constitutionalism or re-constitutionalism is disfavored. Government is best that governs least, so the operation of law is largely negative, to ensure that social and economic liberties are protected from interference. Law functions primarily in a corrective capacity, reacting to wrongs by re-leveling the playing field. Individual autonomy flourishes on liberty, rendering persons responsible for their own choices, whether successful or unsuccessful.

The EU approach to data protection is comprehensive, or omnibus. The Data Protection Directive spans strata of geography, society, and subject matter; the Proposed Regulation will only deepen continental commitment to the confederal system. The system draws its authority initially from fundamental rights as articulated in international human rights instruments and constituting documents. That higher law is then given effect through supranational and national legislation and administrative regulation. Enforcement occurs at all levels from supranational courts to national courts to administrative process. Individuals are entitled to seek redress.

The US approach to data protection is sectoral, or *ad hoc*. Sectoral vectors vary and include dual sovereignty, geographic jurisdiction, scope of regulated industry, and data subject matter. The system has a limited constitutional foundation, especially as against regulated entities in the private sector, and draws its authority principally from sectoral statutes and their regulations. These laws favor paradigms of property and contract, rather than human rights. The statutory framework may be complemented by evolving common law. Enforcement varies with the sectoral scope of the legal device. But enforcement is largely a public undertaking with limited if any redress for individuals.

Macro differences in approach play out in countless ways in the micro systems of data protection. The United States obsession with economic liberty explains the persistent focus on commercial relationships from 2000 Safe Harbor to the 2015 Consumer Privacy Bill of Rights Act. Relationships among persons and commercial actors in the United States are matters of contract and property. The secrecy paradigm arises from the notion of personal data as property. At common law, a person has no persistent legal interest in property that is sold or given away. Moreover, a constitutional right of republication weighs heavily against regulation of information disclosure or transfer. Public actors can be regulated only by the negative operation of constitutional or statutory law. A data processor operates on a presumption of permissibility, subject to highly constrained limitations.

In contrast, Europe's romantic attraction to fundamental rights frames data protection in a rights paradigm. Personal dignity and autonomy are dictated by how information presents one's identity to the world. Accordingly, a person's legal interests persist in information as it flows downstream from one pair of hands to the next. The individual retains rights to direct and control the use of that information, and even to recall it from the marketplace. Positive articulations of human rights imbue government not only with the power to protect those persistent legal rights in information,

but a duty to effect informational rights as against the interests of other actors. Informational rights moreover must be balanced with, and do not yield to, competing rights, such as freedom of expression in republication. Public and private actors alike are bound by the positive operation of law to advance fundamental rights. A data processor operates only with legal authorization, against a background of presumed prohibition.

SAFE HARBOR AND STORMY WEATHER

The patchwork of data protection law in the United States is far from "adequate" to ensure data protection to the standards of the EU Directive. Accordingly, the European Union and United States negotiated a fix in the 2000 Safe Harbor Agreement.[98] To ensure the integrity of data transferred from Directive nations onward to the United States, receiving entities could pledge their allegiance to an agreed on series of principles, including:

- clear **notice** of data collection, processing, and transfer;
- data subject **choice** to opt out (or to opt in when sensitive information is concerned);
- subsequent data **transfer** limited by comparable safeguards;
- reasonable **security** to protect data;
- **relevance** of data processing to purpose of collection;
- data subject **access** to **correct**, amend, or delete data, subject to proportionality of the burden on another's rights;
- **enforcement** through complaint, dispute resolution process, and sufficient sanction.[99]

The mechanism to give force of law to the Safe Harbor Agreement is the broad authority of FTC Act Section 5.[100] A commercial actor must self-certify its compliance to the FTC, and contravention of that representation constitutes an unfair or deceptive trade practice.[101]

Safe Harbor was complemented, if not outstripped, by two other mechanisms for Directive compliance in the United States, model contractual clauses and binding corporate rules. The European Commission approved model contractual clauses in 2001 and 2004.[102] A party in Europe is able to effect a Directive-sanctioned data transfer with a party in the United States by including approved language in a contract governing the transfer.[103] The Article 29 Working Party has approved binding corporate rules in various versions.[104] A multinational corporation may adopt binding corporate rules to effect Directive-sanctioned data transfers between EU and US business components bound by the same rules.[105] Binding corporate rules receive explicit sanction in the Proposed Regulation.[106] Model contractual clauses and binding corporate rules both are made enforceable in the United States through the FTC Act.

Safe Harbor has not been a cure-all. The United States and Europe tussled for years over the US security demand that incoming airliners surrender passenger manifests.[107] But Safe Harbor maintained an uneasy peace for more than a decade. Then European efforts to update data protection law propelled Safe Harbor into renegotiation in 2011.[108] That negotiation was shocked in 2013 by the Snowden revelations of US surveillance practices, causing the European Parliament and national political leaders to scrutinize the renegotiation and raise objections to its singular focus on the private sector.[109]

Nevertheless, negotiators in 2014 announced substantial agreement on revamping Safe Harbor, even while European squabbles persist internally over the Proposed Regulation. Safe Harbor is expected to continue without dramatic change, *i.e.*, without requiring a US consumer privacy bill of rights, or more—save one sticking point. EU leaders desire an individual right of EU citizens to judicial redress in the United States for violations of Safe Harbor commitments, analogous to the right of any person in the European Union dissatisfied with an outcome in a national data protection authority to take the case to court in that nation.[110] The 2000 agreement had solved the enforcement problem with an administrative dispute resolution process only within the FTC. A private cause of action in the third branch of government would introduce a horse of a different color, no less for EU complainants than for the domestic aggrieved. Even the White House's draft CPBRA stops short of private enforcement.

BRIDGE OVER TROUBLED WATER

The competing Atlantic perspectives on data protection must be reconciled to a functional extent.

The difference between the two sides, from a global perspective, is too small to countenance an artificial, legal blockage of the naturally and rapidly increasing fluidity of global exchange in commerce, information, and ideas. In previous writing, I posited that the two systems of privacy and data protection are farther along on a road to convergence than conventional wisdom suggests.[111] But the systems will not harmonize in just the next few years. Some fix of Safe Harbor is needed that both sides can abide.[112]

Following are salient points of difference over data protection that derive from the disparity in legal cultures across the Atlantic. On these points, wisdom counsels agreement to disagree. But the continuation of Safe Harbor requires that these disparities be bridged at least temporarily while the slow but inexorable process of cultural convergence marches on.

US STATE ACTION DOCTRINE VERSUS EU PUBLIC/PRIVATE REGULATION

The state action doctrine and negative operation of the Bill of Rights in the United States continue to mark a bright line in regulation between public and private regulated entities. In the European Union, public and private actors merge as regulated entities under the same data protection rules. The independence principle requires national data protection authorities to work at arm's length from government precisely to ensure non-partisan oversight of the public sector. From a European vantage, the Federal Trade Commission (FTC) is a comfortably non-partisan overseer of the private sector. But Europe evinced frustration, especially after the Snowden revelations, that Department of Commerce authority in data transfer negotiation stopped short of public sector data management. From the outsider's perspective, trusting the Department of Defense to protect personal privacy from public intrusion seems a case of the fox and the henhouse. Worse, this fox bears a sated grin from feasting on cross-border email.

The European perspective here has merit, but only to a point. The dichotomy of state action in the United States is anachronistic. From the perspective of a data subject, privacy is privacy; the secrecy paradigm has merit. The privacy of a library record or a prescription record does not turn on the identity of the snoop. Invasion of privacy injures personal dignity regardless of whether the invader carries official credentials. Moreover, the threat is not dissimilar. The same analytics a retailer uses to generate a customized coupon for cold medicine may be used to track the spread of virus, or to interdict methamphetamine production. Moreover, the same data may be used in the private sector to effect invidious price discrimination[113] or in the public sector to effect discrimination in law enforcement.

So if data protection is the logical extension of privacy rights, the United States cannot justify bearing down on the private sector while handling the public sector with kid gloves. Barring application of the odd sectoral statute, such as the Privacy Protection Act of 1980, which protects journalists,[114] government intelligence gathering and criminal investigation are limited principally by the Fourth Amendment. The "reasonable expectation of privacy" standard, along with its gaping *non sequitur*, the third-party doctrine, is far out of step with contemporary technology. For example, police are now employing "stingray" devices—formerly the province of the super-spy—to mass-capture cell phone data in search of a target. Also the National Security Administration (NSA), reasonably under present law, contends that the mass collection of cell phone and email metadata is permissible under the third-party doctrine. In a speech at Northeastern University Law School in March 2015, Kade Crawford of the Massachusetts ACLU called for *legislative* solutions.[115] She pointed out that the Fourth Amendment merely offers a constitutional floor to protect civil liberties, and the judicial process is far too slow to respond to new technological threats while people's liberty hangs in the balance. Americans should demand legislation to protect civil liberties above the floor, Crawford asserted.

Beyond law enforcement, the Privacy Act of 1974 holds federal government agencies at least to standards that modestly resemble the contemporary fair information practices of Safe Harbor and the European Directive.[116] But the Privacy Act is limited in scope and qualitatively far less stringent. It requires notice that record systems are maintained, but notice means only publication in the *Federal Register*.[117] The Privacy Act prohibits disclosure without consent, but its host of exemptions falls shy of the purpose-driven constraints of the Directive.[118] The Privacy Act affords data subjects rights of access and correction,

though not withdrawal or erasure,[119] and the act vests rights only in citizens and permanent residents.[120]

But when European arguments turn to Snowden, they smack of disingenuity. The Directive itself exempts national security within Europe.[121] The exemption sensibly accommodates national sovereignty in the confederal system and pays faint but apt allegiance to the concept of three pillars in European governance, distinguishing civil, criminal, and military affairs.[122] Foreign intelligence gathering and homeland security in the United States also are rightly distinguished from public record management. Moreover, it strains credulity to imagine that European security officials are not engaged in their own vigorous intelligence gathering. *Der Spiegel* reported that the NSA shared its questionably gotten gains with the German intelligence service.[123] My more erudite colleague Professor David Bender imagined an aid to German Chancellor Angela Merkel tapping her on the shoulder after a speech of US-aimed outrage to politely mention Germany's reliance on the same methods.[124] Whatever national security policy is or should be among the north Atlantic nations, the NSA's most relevant sin might be simply getting caught with its hands in the cookie jar. The contemporary problem of the surveillance state is a problem, and an important one, but it lies well beyond the purview of data transfer policy.

Europe in the end will have to accept the primacy of the public-private distinction in US law and policy. No matter how similar the threat to privacy in each sector, the United States is far from recognizing a merger of public and private for the purpose of data protection regulation. Matters of national security should be relegated, such as the Passenger Name Records Agreement, beyond safe harbor.

At the same time, the United States should look hard at the Privacy Act. Its dated standards, only modestly amended since 1974, hardly suffice to protect personal privacy in the information age. In demonstrating respect for the dignity of the individual, government should set the example for private business, not trail behind. Even pending legislative action, the US executive has ample latitude in its oversight of federal record management to improve information practices with respect to personal privacy. Negotiation over data transfer is an opportunity to learn from comparativism and to improve efficiency and responsiveness in the federal bureaucracy.

The United States also should look hard at the inadequacy of the Fourth Amendment to constrain criminal law enforcement. A bright line does not always separate domestic crime from terroristic threats to national security. But the line shines well enough sometimes, as where the federal preoccupation with drug crime is concerned. Rather than setting a poor example for the states, such as with national security letters that exploit the third-party doctrine, the federal government should lead the way in raising the bar above the Fourth Amendment floor. Again, negotiation over data transfer offers an opportunity to learn from comparative example. And again, the US executive has room to maneuver short of legislation. Attorneys General have ample power to regulate, and have regulated, investigatory practices in federal law enforcement.

US DUAL SOVEREIGNTY VERSUS EU CONFEDERATION

Dual sovereignty under the US Constitution still places sharp limits on the power of the federal government. Especially in the fluid world of contemporary commerce and communication, the brilliance of the 50 state laboratories[125] often is lost on foreign entities, public and private alike, when legal agreements and commercial practices have to adhere simultaneously to the more than 50 standards of US state and territorial governments. But the debated wisdom of continuing this arrangement is immaterial; for better and for worse, it is the constitutional design that will not soon change.

In the European Union, the Directive maintains a confederal separation of powers by vesting data protection authority at the national level.[126] The Proposed Regulation will increase the role of the federal government in the creation of a European Data Protection Board, to enhance consistency across nations. But overall the Proposed Regulation maintains the confederal model of data protection authority. Under the Treaty of Lisbon and the Treaty on the Functioning of the European Union (TFEU),[127] the Proposed Regulation, assuming adoption by the European Council, is within the shared competencies of the European Union and member states,[128] so is consistent with the unique design of vertically separated powers in the European Union. The shared

competence authorizes both social and economic legislation, so there is no distinction in the Directive or the Proposed Regulation between commercial and non-commercial activity. The Directive reaches individuals, if through national data protection authorities, without federalism objections.

Owing in large measure to US federalism, the US legal system is highly resistant to exported EU privacy norms, a source of frustration for EU policy-makers. In the US division of governmental competencies, direct federal power over state governments is nearly restricted to the carrot-and-stick approach. So for the federal government to regulate public sector data protection at the state level would require either a substantial infusion of money or a political willingness to highly rate data protection as prerequisite to some other pot of federal gold—unlikely. With respect to criminal law enforcement, there might be room for Congress to enforce the Fourth Amendment through Fourteenth Amendment incorporation, and the possibility should not be ruled out, especially where equal protection against discrimination is concerned. But the negative operation of the Fourth Amendment still presents an obstacle to positive legislation.

Insofar as data protection in the private sector is predicated on personal privacy, and privacy is understood in the Warren-Brandeis vein, the states possess the broadest authority to regulate. Accordingly, invasion of privacy has developed in state tort law. Even the quasi-intellectual property theory of *post mortem* misappropriation of likeness has been a creation of state statute.[129] Absent recognizable civil rights violation, federal action in the sphere of tort, contract, or property runs against the constitutional grain.

If anything like European shared competence over data protection is to be found in the United States, it is in the regulation of commerce. The broad reach of the Commerce Clause[130]—essentially "substantial effect" doctrine[131] plus the *Wickard* multiplier[132]—allows the federal hand to reach into what otherwise seems to be intrastate commerce. Meanwhile the states have principal regulatory authority over commerce within their borders. As nearly any commercial activity can be said to affect interstate commerce in today's interconnected world, a broad gray zone of concurrent competence lies between the hypothetically purely household activity, on the one side, and federal preemption[133] and the dormant Commerce Clause,[134] on the other. It is no surprise, then, that state experimentation gave rise to the wave of data breach notification laws, inventing a concept that Europe itself has borrowed.[135] Compliance with 47 such laws might vex corporate counsel, but the advent of breach notification laws evidences the state laboratories working as they should.

US federal competence in data transfer negotiation therefore necessarily is limited and finds its most robust expression in the commercial area. Following the Commerce Clause hook, commercial actors are the regulated entities, and the FTC is the logical enforcement authority. The draft CPBRA would bolster the vertical separation of powers by excluding non-commercial individuals and small, therefore more likely intra-state, commercial actors from the scope of regulated entities. The definition of personally identifying information in the draft act similarly maintains focus on the commercial context.

It is unrealistic for Europe to expect that federal data protection in the United States would reach beyond the scope of interstate commerce. If not uniformly, the states have demonstrated a willingness to legislate data protection even more vigorously than the federal government. Massachusetts[136] and California[137] have advanced systems. State experiments in time may percolate to become a more comprehensive federal regulation of commerce. It is moreover disingenuous for Europe to feign ignorance of, or purport disdain for, the federalist competence spheres in the United States. Europe itself is a quasi-federal system with spheres of competence articulated in the TFEU.[138] In fact, customs, market competition, monetary policy, and foreign commerce are set out as areas of exclusive federal competence.[139] So Europe well understands the theory of federalism expressed through the Commerce Clause.

At the same time, the United States should look more carefully at the civil rights implications of inadequate data protection. Galvanized by the war on terror, federal law enforcement and even military authorities have been eager to beef up the capacities of state and local law enforcement with respect to both brute-force gear and technological gadgetry. Little thought has been given to the implications for civil liberties, whether with respect to individuals' physical safety or with respect to personal dignity. The Snowden revelations and recent cases of high technology surveillance by local law enforcement from thermal imaging[140] to GPS[141] to

tower dumps and stingrays[142] are a wake-up call. Recent media attention to police conduct from the killing in Ferguson, Missouri, to the apparent abuse of a University of Virginia student, in the news at the time of this writing[143] point to the dangers of an over-empowered public sector and disparately adverse impact on disadvantaged persons, if not outright discrimination.

In Europe, data protection is working against the tendency of government in the age of terrorism to erect a surveillance state in the name of public security. The relative isolation and sheer size of the United States have tended to forestall the problem of the surveillance state, 9/11 notwithstanding. But the US federal government should be prepared to exercise its power under the Fourteenth Amendment to protect civil rights, recognizing that appropriate data management in both public and private sectors is part of that picture. Negotiation over data transfer is an opportunity, again, to learn from comparativism, and to inspire the federal government to lead the states, rather than trailing behind.

US CONTRACT/PROPERTY PARADIGM VERSUS EU RIGHTS PARADIGM

As explained above, the dominating ethic of personal responsibility in the cultural tradition of US law and policy tends to frame privacy in a paradigm of contract and property. In this paradigm, individuals act affirmatively, to bargain for and protect their own interests. The role of government is to stay out of the way, and the role of law is to make sure that it does. If there is a place for law, it is as a corrective, or remediation, when agreements are broken. Accordingly, personal information is a commodity, and personal data may be sold, licensed, or given away. At the same time, it is extremely difficult to remove and develop data protection, as a subspecies of privacy, from the contract/property paradigm by constitutionalizing it as a fundamental right. Constitutional jurisprudence is text-based and interpretive, so fundamental rights tend to be defined statically.

In contrast, the dominating ethic of social responsibility in the cultural tradition of law and policy in post-World War II Europe tends to frame privacy in a paradigm of human rights. In this paradigm, individuals are entitled passively to some protection of their interests by the state and by their fellow citizens. The role of government is to act affirmatively to ensure the realization of human rights, and the role of law is to give effect to rights in everyday life. Law acts as a distributive, or allocative, force, organizing the resources of society to maximize each individual's potential. Accordingly, personal information is an expression of identity, and personal data may be shared, but remains an aspect of personhood, under the control of the originator. Data protection is recognized as a fundamental right, a subspecies of privacy, in the constituting instruments of the European Union. Constitutional jurisprudence is interpretive, but adaptive and evolving, so fundamental rights may grow dynamically.

The most evident manifestation of this disparity in approach to data protection is in each continent's permissiveness of an individual's control over downstream use and transfer of personal information. In the United States, downstream control is a nearly foreign concept, as unlikely as a former homeowner returning to the home to object to the new owner's décor. Personal data are an alienable commodity. In the European Union, however, an individual's surrender of personal information for unrestrained downstream use is no more legally permissible than surrendering one's liberty to involuntary servitude. Personal data are integral to individual identity and cannot be alienated.

This disparity is perhaps the most toxic in trans-Atlantic negotiation, because it derives from the very identity of each culture. To American eyes, the European system seems the pandering of a nanny state determined to interject behemoth government into every human interaction to ensure that no sloth goes unrewarded, that no human endeavor goes unpunished, and that mankind's natural Darwinist drive to improve the human condition through productive achievement is utterly derailed. To European eyes, the US system seems a hopeless cult of delusional majoritarianists held unwitting captive to the almighty dollar and possessed of an inexplicably messianic conviction that all the world's people will be better off once recruited into zombie servitude to corporate overlords.

This is a gap not easily bridged. With blunt cudgel of human rights, Europe will only reinforce the worst of US anxieties. Rather, I propose that the start of an answer lies in the Fourth Amendment itself.

If the minimal standard of tolerable intrusion into a person's life is guided by *reasonableness*—whether the *reasonable* expectation of the individual, or the *reasonable* suspicion of the state—perhaps it is that same standard that can help Americans find their way to a new norm of privacy.

Critics of the Fourth Amendment standard aptly assert that the problem with reasonableness is its malleability *downward*, that is, to a lowest common denominator of tolerable conduct. But there is no reason that reasonableness always must evolve downwardly. In tort law, reasonableness, as the keystone of breach in negligence, has been well known to evolve *upwardly*. Conduct that was once regarded as comfortably within the purview of the "reasonable man"—who in the 1920s apparently "[got] out of his car at every railroad crossing to check for oncoming trains"[144]—is now regarded as unexpected of the "reasonable person," whose very name has adapted to new norms.[145] Is the beauty of the Fourth Amendment not in the word "unreasonable"?[146]

The same concept might unlock a new future for data protection in the private sector. The presently recent movement to piggyback negligence for data protection offenses on sectoral privacy statutes with no private cause of action is indicative of the capacity of the common law to evolve and recognize civil wrongs in unprecedented circumstances. Reasonableness lies at the heart of general negligence, and negligence *per se* permits, in most jurisdictions, the substitution of the statutory violation. In an alternative formulation of negligence *per se*, the statutory violation is at least admissible as persuasive evidence for the finder of fact on the core question of breach. Either way, the common law seems to have detected a sensible connection between expectation in data protection law and standards of reasonable conduct. In the same vein, 2014 saw the adoption of a new common law tort in UK courts: the misuse of private information.[147] Seeming to lie somewhere between conventional negligence and breach of confidential duty,[148] the nascent creature is still taking shape. Just as the negligence theory in the United States, the new British tort drew breath from breach of data protection standards[149]—despite the Brits' famous hostility to aggressive federalism in the European data protection system.[150]

Even in the contract/property paradigm, tort law and civil rights play referee in private and public sector respectively. The duplication of tort norms in civil rights, where private causes of action cannot be denied upon a failure of legislative authorization, demonstrates the common role. Tort steps in to maintain a normative floor of social behavior where contract and property law fail, as when a contract or property transfer is procured by fraud, or a place of employment is not maintained to a reasonable standard of safety. The civil rights action provides the same floor where the defendant acts under color of law and violates a constitutional norm.[151]

It is premature for Europe to expect private judicial redress for victims of data protection in the United States, for any plaintiff, much less a European plaintiff. But given a little more time, the patchwork of US sectoral law, including the common law, might get there itself. Forty-seven states have adopted data breach notification laws, 14 with a private cause of action.

Lest there be any doubt that our tort friend *reasonableness* is up to the job of data protection, "reasonable" or "reasonably" appears 47 times in the CPBRA.

CONCLUSION

The EU and US data protection systems differ in important ways. The EU system is omnibus, or comprehensive, and derives from the social-democratic tradition of European governance. The US system is sectoral and accords with the libertarian tradition in US law and policy. For more than a decade, these systems have co-existed with open channels for data transfer under the Safe Harbor Agreement and related model contractual clauses and binding corporate rules. Now those open channels are threatened in a safe harbor renegotiation necessitated by rapidly advancing technology, evolving social norms, and a legal system trying to keep up with those changes.

The cultural gulf in privacy law and policy between the United States and Europe will not be bridged by a data protection agreement. In the long term, the United States and Europe might move naturally into harmonization. But in the short term, a continuing accommodation is required, lest the continents' differences impede technological, social, and economic growth. To advance this understanding,

this article highlighted three salient differences between the US and EU law and policy.

First, the US state action doctrine drives a US data protection system to be different from the EU system, in which public and private sectors merge as regulated entities. In this respect, Europe will have to accept the public-private distinction in the United States and embrace the dichotomy of negotiating partners. In turn, the United States must be willing to examine seriously, and to consider remediating, the shortcomings of the Privacy Act and the Fourth Amendment as regulations of public sector data protection, just important as regulation of the commercial sector.

Second, US dual sovereignty drives an approach to data protection different from the confederal approach of the EU Data Protection Directive and Proposed General Data Protection Regulation. It is unrealistic at present for Europe to expect that federal data protection in the United States will reach beyond the scope of interstate commerce. But if afforded breathing room, the US states will in time develop more advanced models for data protection. In turn, the United States must be willing to consider the civil rights implications of inadequate data protection in private and public sector, and to consider how federal power may be used appropriately to avert the construction of a surveillance state.

Third, the contract/property paradigm controls the legal character of personal data in the United States, while in Europe, a rights paradigm prevails. These paradigms drive very different data protection systems that arouse impassioned defenders on each side. While this cultural gap will not be bridged easily or quickly, convergence over time is likely. Europe is unlikely now to secure private legal redress for EU citizens in the next iteration of safe harbor. But recent developments in US law suggest that experimentation with data protection statutes and tort law will move the United States toward a more dynamic understanding of privacy. Corrective remedies for American and Europeans alike might lie just over the horizon.

NOTES

1. Directive 95/46/EC of the European Parliament and the Council 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, *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF* [hereinafter Directive].
2. *See* U.S. Department of Commerce, Safe Harbor Home, *http://www.export.gov/safeharbor/index.asp*.
3. Samuel D. Warren & Louis D. Brandeis, "The Right to Privacy," 4 *Harv. L. Rev.* 193, 193 (1890).
4. Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810 at 71 (1948).
5. Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 222.
6. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Eur. T.S. No. 108 [hereinafter Convention 108]. Convention 108 is open to signatories worldwide, not just in Europe, and remains in force today as the only global instrument concerning data protection. Electronic Information Privacy Center, Council of Europe Privacy Convention, *https://epic.org/privacy/intl/coeconvention/* (last visited Mar. 21, 2015).
7. Convention 108, *supra* n.6, pmbl.
8. *Id.* pmbl. & art. 1.
9. *Id.* arts. 9, 12, 13.
10. Charter of Fundamental Rights of the European Union, art. 7, 2000 O.J. (C 364) 18 [hereinafter Charter].
11. Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Communities, Dec. 13, 2007, O.J. (C 306) [hereinafter Treaty of Lisbon].
12. Charter, *supra* n.10, art. 52(3).
13. EU Network of Independent Experts on Fundamental Rights, Commentary of the Charter of Fundamental Rights of the European Union 90 (2006), *http://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf*.
14. European Commission, EU Charter of Fundamental Rights, *http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm* (last visited Mar. 21, 2015).
15. *See also* Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37. *See generally* European Commission, Protection of Personal Data, *http://ec.europa.eu/justice/data-protection/index_en.htm* (last visited Mar. 21, 2015).
16. *E.g.*, Paul Schwartz, "The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures," 126 *Harv. L. Rev.* 1966, 1971-1979 (2013).
17. Directive, *supra* n.1, art. 2(a).
18. *Id.* art. 2(b).
19. *Id.* art. 2(d)-(e).
20. *Id.* art. 7.
21. European Commission, Commission Staff Working Paper: Impact Assessment, SEC(2012) 72 final (Jan. 25, 2012), annex 4, § 1.2, *http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf* (PDF page 161).
22. Directive, *supra* n.1, art. 6.
23. *Id.* art. 12.
24. *Id.* arts. 10-11.
25. *See id.* arts. 12(a), 15(1) (restricting automated processing).
26. *Id.* art. 2(h).
27. *Id.* pmbl. ¶ 70.
28. *Id.* art. 8 ("personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and … concerning health or sex life").
29. *Id.* art. 17.
30. *Id.* art. 28.

31. *Id*. art. 28(1).
32. *Id*. art. 25.
33. *Id*. art. 13.
34. *Id*. art. 3.
35. Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM (2012) 11 final (Jan. 25, 2012) [hereinafter Proposed Regulation], *http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf*.
36. European Parliament Legislative Resolution of March 12, 2014 on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM(2012)0011–C7-0025/2012–2012/0011(COD), *http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN*.
37. *See*, *e.g.*, Francoise Gilbert, "European Data Protection 2.0: New Compliance Requirements in Sight—What the Proposed EU Data Protection Regulation Means for U.S. Companies," 28 *Santa Clara Computer & High Tech. L.J.* 815, 827-862 (2012); Richard J. Peltz-Steele, "The New American Privacy," 44 *Geo. J. Int'l L.* 365, 373-383 (2013).
38. Proposed Regulation, *supra* n.35, art. 3(2).
39. The Thirteenth Amendment is exceptional in this regard, but its textual scope is narrow.
40. Stenberg v. Carhart, 530 U.S. 914, 921 (2000).
41. Cruzan *ex rel.* Cruzan v. Director, Mo. Dept. of Health, 497 U.S. 261, 278 (1990).
42. Washington v. Glucksberg, 521 U.S. 702, 723 (1997).
43. U.S. v. Jones, 132 S. Ct. 945, 950 (2012).
44. *E.g.*, Thomas Y. Davies, "Recovering the Original Fourth Amendment," 98 *Mich. L. Rev.* 547, 731-734 (1999) (describing "relativistic 'reasonableness'" in contrast with original meaning).
45. *E.g.*, Kade Crawford, Director of Technology for Liberty Program of ACLU of Massachusetts, Keynote Speech at Symposium: Information and Data in the Era of Accessibility, Northeastern University Law Journal, Boston, Mass., Mar. 13, 2015.
46. Smith v. Md., 442 U.S. 735, 743-744 (1979).
47. Daniel J. Solove, "Access and Aggregation: Public Records, Privacy and the Constitution," 86 *Minn. L. Rev.* 1137, 1140-1141 (2002); *see also* Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age 42-44 (2004).
48. Whalen v. Roe, 429 U.S. 589 (1977).
49. Nixon v. Administrator of Gen. Servs., 433 U.S. 425 (1977).
50. NASA v. Nelson, 562 U.S. 134 (2011).
51. U.S. Const. art. I, § 8, cl. 3.
52. 15 U.S.C. §§ 1681–1681x (2011).
53. 20 U.S.C. § 1232g (2013).
54. 5 U.S.C. § 552a (2010).
55. 18 U.S.C.A. § 2710 (2013).
56. Pub. L. No. 104-191, 110 Stat. 1936.
57. 15 U.S.C. §§ 6501-6506.
58. *See generally* U.S. Department of Education, Family Educational Rights and Privacy Act, *http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html* (last visited Mar. 21, 2015).
59. Beatriz Costa-Lima, "FERPA Amendment Would Establish 'Safeguards' for Student Data Privacy," *Student Press L. Center*, Nov. 10, 2014, *http://www.splc.org/article/2014/11/ferpa-amendment-would-establish-safeguards-for-student-data-privacy*.
60. *See generally* U.S. Department of Health & Human Services, Health Information Privacy, *http://www.hhs.gov/ocr/privacy/* (last visited Mar. 21, 2015).
61. *See* U.S. Department of Health & Human Services, Health Information Privacy, *http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html* (last visited Mar. 21, 2015).
62. National Conference of State Legislatures, Security Breach Notification Laws, *http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx* (updated Jan. 12, 2015; last visited Mar. 21, 2015). There are at the time of this writing no such laws in Alabama, New Mexico, and South Dakota. *Id*.
63. Baker & Hostetler, Data Breach Charts 14-15 (2014), *http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf*.
64. Pub. L. No. 106-102, 113 Stat. 1338 (1999). *See generally* Federal Trade Commission, In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act, *https://www.ftc.gov/tips-advice/business-center/guidance/brief-financial-privacy-requirements-gramm-leach-bliley-act* (last visited Mar. 21, 2015).
65. Cory Bennett, "Lawmakers *See* Momentum for Data Breach Legislation," *Hill*, Jan. 27, 2015, *http://thehill.com/policy/cybersecurity/230867-data-breach-bill-is-achievable-goal*.
66. 15 U.S.C. § 45(a)(1).
67. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014).
68. The Third Circuit heard oral argument on March 3, 2015. Electronic Privacy Information Center, FTC v. Wyndham, *https://epic.org/amicus/ftc/wyndham/* (last visited Mar. 21, 2015).
69. *E.g.*, Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 102 A.3d 32, 49 (Conn. 2014).
70. *Id.*; *see also* Hopkins v. Kay, 2014 O.N.C.A. 514 (Ontario Ct. App. 2014) (finding provincial privacy law not preemptive of class privacy claim against hospital).
71. White House, Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015 (Feb. 27, 2015) [hereinafter CPBRA], *https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf*.
72. White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (2012), *http://www.whitehouse.gov/sites/default/files/email-files/privacy_white_paper.pdf*.
73. CPBRA, *supra* n.71, § 4(b)(1).
74. *Id*. § 201.
75. *Id*. § 202.
76. *Id*. § 4(a).
77. *Id*. § 4(b). Also excluded are entities of fewer than 26 employees if data processing is limited to hiring and employment. *Id*. § 4(b)(1)(E).
78. *Id*. § 203.
79. *Id*. § 4(k).
80. *Id*. § 104.
81. *Id*. § 101 ("in concise and easily understandable language, accurate, clear, timely, and conspicuous").
82. *Id*. § 102.
83. *Id*. § 103.
84. *Id*. § 102.
85. *Id*. § 106.
86. *Id*. § 104(b).

87. *Id.* §§ 105, 107.
88. *Id.* § 103(b).
89. *Id.* § 301.
90. *Id.* § 106(b)(2).
91. *Id.* §§ 102(c)(3)(A), 106(a)(2)(B), 106(c)(3)(A), 404(a).
92. *See* Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2667 (2011).
93. Wendy Davis, "Advocates Say White House Privacy Proposal Filled with Loopholes," MediaPost, Feb. 27, 2015, *http://www.mediapost.com/publications/article/244720/advocates-say-white-house-privacy-proposal-filled.html* (*quoting* Justin Brookman, director of consumer privacy at Center for Democracy and Technology).
94. *Id.* (*quoting* Markey).
95. *Id.* (*quoting* Mike Zaneis, general counsel for Interactive Advertising Bureau).
96. *See*, *e.g.*, Ioanna Tourkochoriti, "The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide between U.S.-EU in Data Privacy Protection," 36 *U. Ark. Little Rock L. Rev.* 161, 164-175 (2014).
97. This point is not new, and I join a long line of observers. For a dated but still apt and highly sophisticated analysis, *see* Joel R. Reidenberg, "Resolving Conflicting International Data Privacy Rules in Cyberspace," 52 *Stan. L. Rev.* 1315 (2000).
98. U.S. Department of Commerce, Safe Harbor Privacy Principles, *http://www.export.gov/safeharbor/eu/eg_main_018475.asp* (issued July 21, 2000; last updated Jan. 30, 2009; last visited Mar. 21, 2015). *See generally* U.S. Department of Commerce, Safe Harbor Home, *http://www.export.gov/safeharbor/index.asp* (last visited Mar. 21, 2015).
99. U.S. Department of Commerce, Safe Harbor Privacy Principles, *supra* n.98.
100. 15 U.S.C. § 45.
101. *See* U.S. Department of Commerce, U.S.-EU Safe Harbor Framework: A Guide to Self-Certification (2009), *http://www.export.gov/build/groups/public/@eg_main/@safeharbor/documents/webcontent/eg_main_061613.pdf* (updated March 2013).
102. European Commission Decision C(2004)5721, *http://ec.europa.eu/justice/data-protection/document/international-transfers/files/clauses_for_personal_data_transfer_set_ii_c2004-5721.doc*; European Commission Decision 2001/497/EC, *http://ec.europa.eu/justice/data-protection/document/international-transfers/files/clauses_for_personal_data_transfer_set_i_2001-497-ec.doc*.
103. *See generally* European Commission, Model Contracts for the Transfer of Personal Data to Third Countries, *http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm* (last visited Mar. 21, 2015).
104. *See generally* European Commission, Overview on Binding Corporate Rules, *http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm* (last visited Mar. 21, 2015).
105. *Id.*
106. Proposed Regulation, *supra* n.35, art. 43.
107. *See generally* European Commission, Transfer of Air Passenger Name Record (PNR) Data and Terrorist Finance Tracking Programme (TFTP) (US), *http://ec.europa.eu/justice/data-protection/document/international-transfers/pnr-tftp/pnr-and-tftp_en.htm#h2-3* (last visited Mar. 21, 2015).
108. *See generally* European Commission, Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 final (Nov. 27, 2013), *http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415704124887&uri=CELEX:52013DC0847*.
109. In a non-binding and effectively symbolic vote, the European Parliament voted after the revelation of the US surveillance program to suspend the Safe Harbor agreement with the United States. European Parliament, US NSA: Stop Mass Surveillance Now or Face Consequences, MEPs Say (Dec. 3, 2014), *http://www.europarl.europa.eu/news/en/news-room/content/20140307IPR38203/html/US-NSA-stop-mass-surveillance-now-or-face-consequences-MEPs-say*.
110. European Commission, Factsheet EU-US: Negotiations on Data Protection 2-3 (2014), *http://ec.europa.eu/justice/data-protection/files/factsheets/umbrella_factsheet_en.pdf*.
111. Peltz-Steele, *supra* n.37, at 394-404.
112. Professor Paul Schwartz and Daniel Solove proposed an inventive stop-gap. *See* Paul M. Schwartz & Daniel J. Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information," 86 *N.Y.U. L. Rev.* 1814 (2011).
113. *See generally* White House, Big Data and Differential Pricing (Feb. 2015), *https://www.whitehouse.gov/sites/default/files/docs/Big_Data_Report_Nonembargo_v2.pdf*.
114. 42 U.S.C. §§ 2000aa to 2000aa-12 (1996).
115. Crawford, *supra* n.45.
116. *See* 5 U.S.C. § 552a.
117. *Id.* § 552a(e).
118. *Id.* § 552a(b), (j), (k).
119. *Id.* § 552a(d).
120. *Id.* § 552a(a)(2).
121. Directive, *supra* n.1, art. 13(1).
122. The Treaty of Lisbon, *supra* n.11, abandoned the three-pillars concept, but it remains informative to understand the current quasi-federal structure of the European Union.
123. "'Prolific Partner': German Intelligence Used NSA Spy Program," *Spiegel*, July 20, 2013, *http://www.spiegel.de/international/germany/german-intelligence-agencies-used-nsa-spying-program-a-912173.html*.
124. David Bender, "Which Regime Offers More Actual Privacy—US or EU?," 2014 *Emerging Issues* 7189; *see also* David Bender, Presentation: E.U. or the U.S.: Which Has More Actual Privacy?, at Symposium: Information and Data in the Era of Accessibility, *Northeastern University Law Journal*, Boston, Mass., Mar. 13, 2015.
125. The concept derives from New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).
126. I recognize that the European Union has a hybrid model of government, not purely federation and not purely confederation. The way the data protection system is organized leans to the confederal side, so I elect that term.
127. Treaty on the Functioning of the European Union, 2012 O.J. (C 326) 47, art. 4, *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012E/TXT* [hereinafter TFEU].
128. *See* European Commission, European Citizens' Initiative: FAQ on the EU Competences and the European Commission Powers, *http://ec.europa.eu/citizens-initiative/public/competences* (last visited Mar. 21, 2015).
129. *See* Jonathan Faber, Right of Publicity Statutes, *http://rightofpublicity.com/statutes* (last visited Mar. 21, 2015).
130. U.S. Const. art. I, § 8, cl. 3.
131. Gonzales v. Raich, 545 U.S. 1, 17 (2005).
132. Wickard v. Filburn, 317 U.S. 111, 127-128 (1942).
133. U.S. Const. art. 6, cl. 2.
134. Department of Revenue v. Davis, 553 U.S. 328, 337-338 (2008).
135. *See* Proposed Regulation, *supra* n.35, art. 32.
136. Mass. Gen. L. § 93H; 201 Mass. Code Regs. 17.01-.05.
137. *See generally* California Office of the Attorney General, Privacy Enforcement and Protection, *http://oag.ca.gov/privacy* (last visited Mar. 21, 2015).

138. *See* European Commission, European Citizens' Initiative: FAQ on the EU Competences and the European Commission Powers, *supra* n.128.

139. TFEU, *supra* n.127, art. 3.

140. Kyllo v. U.S., 533 U.S. 27, 29-30 (2001).

141. U.S. v. Jones, 132 S. Ct. 945, 948-949 (2012).

142. In re Cell Tower Records under 18 U.S.C. § 2703(D), No. H-15-136M, ___ F. Supp. 3d ___, 2015 WL 1022018, at *2-*4 (S.D. Tex. Mar. 9, 2015).

143. Terrance F. Ross, "When Police Misconduct Transcends Class," *Atlantic*, Mar. 20, 2015, *http://www.theatlantic.com/education/archive/2015/03/the-transcendence-of-police-misconduct/388168/*.

144. Randy T. Austin, "Better Off with the Reasonable Man Dead or the Reasonable Man Did the Darndest Things," 1992 *B.Y.U. L. Rev.* 479, 489 (1992) (*citing* Baltimore O.R.R. v. Goodman, 275 U.S. 66, 69 (1927)).

145. *Id.* at 482.

146. *See* Davies, *supra* n.44, at 747 (favorably regarding evolving understanding even if inconsistent with original meaning).

147. Vidal-Hall v. Google Inc., [2014] EWHC 13, ¶ 70 (Q.B.), available at *http://www.bailii.org/ew/cases/EWHC/QB/2014/13.html*.

148. *See id.* ¶ 59.

149. *See id.* ¶¶ 37, 89-94.

150. *See* Stuart Lauchlan, "It's European Dis-Union," *Raconteur*, Dec. 10, 2014, *http://raconteur.net/technology/its-european-dis-union*.

151. 42 U.S.C. § 1983 (1996).