2017

Ancient Worries and Modern Fears: Different Roots and Common Effects of U.S. and E.U. Privacy Regulation

Pierluigi Perri

CONNECTICUT
LAW REVIEW

VOLUME 49 SEPTEMBER 2017 NUMBER 5

Article

Ancient Worries and Modern Fears: Different Roots and Common Effects of U.S. and E.U. Privacy Regulation

PIERLUIGI PERRI AND DAVID THAW

Much legal and technical scholarship discusses the differing views of the United States and European Union toward privacy concepts and regulation. A substantial amount of effort in recent years, in both research and policy, focuses on attempting to reconcile these viewpoints searching for a common framework with a common level of protection for citizens from both sides of Atlantic. Reconciliation, we argue, misunderstands the nature of the challenge facing effective cross-border data flows. No such reconciliation can usually occur without abdication of some sovereign authority of nations, which would require the adoption of an international agreement with typical tools of international law. In this Article, we explore an alternative means to achieve effective data interchange governance among the Western nations, arguing that the focus for addressing privacy issues created in cross-border data flows should instead be procedural, rather than substantive.

Beginning with the observation that both U.S. and E.U. cultures share a common fear of "chilling effects" infringing various rights to privacy, we link the differences in privacy fears to the comparative views of the role of the state. These differences are instructive in that while they limit the potential for substantive harmonization of privacy goals, they also create substantial opportunity for procedural harmonization.

Such procedural harmonization would afford many benefits, reducing transaction costs for multi-national organizations and increasing the probability that individuals can express (and rely upon implementation) of their privacy preferences The result is a system we describe as Market-Supervised Regulatory Delegation, in which the substantive differences among nations can be respected and implemented in an international market for expressing privacy preferences that is not distorted by the overhead of competing compliance regimes.

ARTICLE CONTENTS

INTRODUCTION 1623

I. DIFFERENT ORIGINS OF U.S. AND E.U. FEDERALISM AS CAUSES OF DIFFERENT PERCEPTION OF PRIVACY VALUE . 1624

- A. BRIEFLY ABOUT THE ADMINISTRATIVE STATE IN THE UNITED STATES 1626
- B. BRIEFLY ABOUT THE ADMINISTRATIVE STATE IN THE EUROPEAN UNION 1630

II. DEFINING THE IDEA (NOT THE LAW) OF PRIVACY FOR U.S. AND E.U. CITIZENS: SIMILITUDES AND DIFFERENCES 1633

- A. THE CONCEPT OF "CHILLING EFFECTS" 1633
- B. OVERVIEW OF U.S. PRIVACY REGULATION 1635
- C. OVERVIEW OF E.U. PRIVACY REGULATION 1639
- D. U.S. – E.U. SHARED COMMITMENTS 1644

III. COMMON GROUND IN U.S. AND E.U. BUREAUCRATIC ORGANIZATION: UNIFYING PRIVACY REGULATION— "MARKET-SUPERVISED REGULATORY DELEGATION" 1647

- A. FEDERATED REGULATION (MANAGEMENT-BASED REGULATORY DELEGATION) 1648
- B. FEDERATED REGULATION SUPPORTS NATIONAL COORDINATION TOWARD HARMONIZED PRIVACY PROCESSES 1649
- C. FEDERATED REGULATION FOR STANDARDIZING COMPLIANCE BY REGULATED ENTITIES 1651

IV. A PROPOSAL FOR IMPLEMENTATION 1652

CONCLUSION 1654

Ancient Worries and Modern Fears: Different Roots and Common Effects of U.S. and E.U. Privacy Regulation

PIERLUIGI PERRI AND DAVID THAW [*]

INTRODUCTION

The idea that the U.S. and E.U. have different perceptions about privacy values is widespread. When describing the U.S. view, much scholarship starts from Warren and Brandeis' Article, *The Right to Privacy*, which presents a view of "the right to be let alone" very different from common European perception of privacy.[1] This focus on substantive difference, however, overlooks other differences that may explain why these two contemporary western cultures developed such different views of the right to privacy. This Article compares the differing perceptions of privacy through the lens of causation, tracing those perceptions' roots along with the development of the administrative state in each region. The privacy "worries" resulting from violations of the two different perceptions are, in fact, quite similar in quality and differ not in the resultant fear but rather in the respective societies' views of the role of regulation.

Contemporary examinations of privacy law in the United States and the European Union focus predominantly on the substantial differences between these regulatory regimes and the strength of protection they afford. This comparative view correctly describes the different actors with which each regime's privacy protections are concerned: the U.S. regime fears intrusions by the State, whereas the E.U. regime fears intrusions by private corporations, especially so-called Big Data corporations. The traditional view, however, is incomplete because it overlooks a critical commonality between the two regimes—the shared fear of what bad actions the "privacy

---

[*] Pierluigi Perri is an Associate Research Professor of Advanced Computer Law at Università degli Studi di Milano (University of Milan). David Thaw is an Assistant Professor of Law and Information Sciences at the University of Pittsburgh. Both authors are Affiliated Fellows of the Information Society Project at Yale Law School, and their names are listed in alphabetical order. This Article has been produced with the assistance of the European Union. The contents of this Article are the sole responsibility of Pierluigi Perri and David Thaw, and can in no way be taken to reflect the views of the European Union. The authors are grateful for the support of The European Studies Center at the University of Pittsburgh, a Jean Monnet Center of Excellence. The authors also thank the Università degli Studi di Milano for its support of this work. This Article benefitted from the thoughtful commentary of Jack Balkin and Guido Calabresi.

[1] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193, 206 (1890) (describing the evolution of recognized personal rights, particularly, the "right to be let alone").

intruder" will take. Specifically, while each regime fears different actors—both are concerned about the "chilling effects" on individual freedoms that would result from privacy invasions.

The common values inherent in both United States and European Union privacy regulation, and in their associated bureaucratic institutions, provide clues to developing a framework for coordinating these two different regulatory regimes. Such coordination has many benefits for international data flow, which has become a fact of modern life. Multi-national organizations, for example, handle vast amounts of data and compliance with different regulatory procedures can be highly inefficient. The application of Management-Based Regulatory Delegation theory, or "Federated Regulation," can allow individual states to maintain their autonomy with respect to substantive privacy values while reducing compliance costs by coordinating procedural regulatory processes. Such an approach is possible because of the common shared fear among U.S. and E.U. States—that privacy invasions, regardless of their source, will ultimately lead to chilling effects on individual action.

The resultant approach, which we describe as Supervised Market-Based Regulation, allows for an international regulatory framework which both shows respect for national differences in privacy preferences while allowing for harmonized compliance procedures which reduce barriers to free flow of information and discourage compliance-avoidance activities.

I. DIFFERENT ORIGINS OF U.S. AND E.U. FEDERALISM AS CAUSES OF DIFFERENT PERCEPTION OF PRIVACY VALUE

This Section explores the different ways in which the federalist systems of the U.S. and E.U. affect perceptions of privacy. Views of the State as instrumentalist in Europe (fearing unrestrained private action) and views of the State as self-limiting in the U.S. (fearing unrestrained state action) accord with the classic fears each society's government seeks to restrain. These views still predominate modern political discourse and, we argue, translate into modern conceptions of the role of privacy regulation in the two respective societies.

U.S. political discourse focuses far more on concerns regarding privacy intrusions by state actions than it does on privacy intrusions by private corporations. E.U. political discourse, by contrast, focuses far more on privacy intrusions by private corporations than does U.S. political discourse. Furthermore, notwithstanding substantial political disagreement among U.S. states and regions, and among E.U. member states, the two comparative dimensions described above are among the few aspects of privacy about which there is agreement within each respective culture. U.S. states and regions generally agree that unrestrained federal power threatens privacy, and E.U. members states generally agree that unrestrained capitalism

threatens privacy.[2]

In this regard, the U.S. and E.U. irreconcilably differ as to who are the "feared privacy invader(s)." U.S. culture "fears" government invasion and specifically protects against it,[3] looking to the private market as an instrument to protect privacy choices. E.U. culture "fears" invasions by private corporations (sometimes referred to as "imported capitalism" especially as respects U.S. technology companies) and looks to Data Protection Authorities as instruments to issue guidelines or even binding regulation that protect privacy choices[4].

These irreconcilable differences make *substantive* convergence between U.S. and E.U. privacy regulation deeply problematic. Even if recent responses by E.U. governments to national security and terrorism events were to raise fears of privacy invasion by national governments, as some have recently observed,[5] such a choice would do little to suppress fears of private corporate action. The fundamental difference regarding the instrumentalities of preference expression and free-choice preservation would remain.[6]

Curiously, however, each of these two societies shares a common fear—the *result* that will manifest as consequence of failing to protect against violations of individuals' privacy. Each society shares the belief that privacy invasions, or perhaps more importantly *perceptions of risk of privacy invasions*, will deter individual action and expression creating the normalizing effects predicted by Foucault.[7] A particularly salient example of this shared fear is highlighted by responses on both sides of the Atlantic

---

[2] Such a distinction is not unsurprising, particularly in the privacy context, considering the social and historical roots of American and European societies as placing greater value on "individualism" and "order and rank" respectively. William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 965–966 (2016).

[3] *E.g.,* U.S. Const, amend. IV; William J. Cuddihy, *The Fourth Amendment. Origins and Original Meaning*, OXFORD UNIV. PRESS. (2009). *See also, e.g.,* Riley v. California, 134 S.Ct. 2473, 2494–95 (2014); *see also generally* Griswold v. Connecticut, 381 U.S. 479 (1965).

[4] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy in Europe: Initial Data on Governance Choices and Corporate Practices*, 81 GEO. WASH. L. REV. 1529, 1644–1648 (2013); Francesca Bignami, *Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy*, 59 AM. J. COMP. L. 2, 441–457 (2011).

[5] *See The Terrorist in the Data*, ECONOMIST (Nov. 26, 2015), http://www.economist.com/news/briefing/21679266-how-balance-security-privacy-after-paris-attacks-terrorist-data (discussing digital privacy concerns following the implementation of new security programs after the Paris attacks).

[6] It is important to note that the distinction drawn here, and throughout this Article, is *not* that European citizens are unconcerned with State-based privacy intrusions. Quite the opposite: after World War II, many (now) EU nations implemented specific safeguards against such intrusions in their respective codes. Rather, instead, what we distinguish here is the current primary focus of *unaddressed* (or under addressed) privacy concerns of the respective polities in contemporary society.

[7] *See* MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 200–01 (Alan Sheridan trans., Vintage Books 2d ed. 1995) (exploring a hypothetical society where public perception of "permanent visibility . . . assures the automatic functioning of power").

in recent years to bulk data collection through classified government surveillance programs.[8] This shared concept of "chilling effects"[9] gives hope that while substantive convergence in transatlantic privacy regulation is unlikely, perhaps these limited shared values might facilitate *procedural* harmonization in privacy regulation.

It is useful, at this point, to briefly trace the histories of the administrative states in the U.S. and the E.U., focusing on their respective fears of unrestrained state action and unrestrained "imported capitalism," and then examine how the commonalities within the respective regulatory systems make possible a form of procedural harmonization when viewed from the perspective of the shared desire to prevent chilling effects on individual action.

A. *Briefly about the Administrative State in the United States and the regulation of privacy*

The concept of the administrative state—if contemplated at all by the Framers during the Constitutional Convention—was at most a side thought viewed as wholly manageable by a single Chief Executive.[10] What *was* clearly at the forefront of the Framers' concerns was a deep-seeded fear of the encroachment of individuals' freedoms by the State. This fear was evident in the references to substantial dissatisfaction with and concern about the arbitrariness of the British monarchic system.[11]

In forming the new Republic, the Framers' fear of state privacy invasion was also evident in debates regarding the division of power between the federal and state governments. While reservation of the power to state governments might be interpreted as not fearful of governmental abuse, both historical argument and structural analysis suggest otherwise. First, as a structural matter, the giving over of power to a national government was a more lasting and difficult-to-alter proposition for the citizens of the late 1700s than was maintaining their individual state governments. John DeWitt's Letter of October 27, 1787 calls for caution and notes that the powers of that new government will not be reconstituted annually, but are designed to endure perpetually and thus calls upon his fellow citizens to

---

[8] *See* Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C.L. REV. 609, 680 (2007).

[9] *See* Yoan Hermstrüwer & Stephan Dickert, *Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten*, MPI COLLECTIVE GOODS PREPRINT, No. 2013/15 (2013).

[10] *See* Peter L. Strauss, *Formal and Functional Approaches to Separation-of-Powers Questions—A Foolish Inconsistency?*, 72 CORNELL L. REV. 488, 492–93 (1987) ("If in 1787 such a merger of [governmental powers and] functions was unthinkable, in 1987 it is unavoidable given Congress's need to delegate at some level the making of policy . . . .").

[11] *See* RALPH KETCHMAN, THE ANTI-FEDERALIST PAPERS AND THE CONSTITUTIONAL CONVENTION DEBATES 1–6 (1986) (discussing the Framers' dissatisfaction with the British monarchy and attempts to form a better government).

exercise great care in considering its adoption.[12] In particular, DeWitt notes "[t]hat insatiable thirst for unconditional control over our fellow creatures . . . produced the first Bill of Rights ever prefixed to a Frame of Government."[13] The position DeWitt represents, however, did not view the Bill of Rights as a complete solution:

> The people, although fully sensible that they reserved every title of power that they did not expressly grant away, yet *afraid that the words made use of*, to express those rights so granted might convey more than originally intended, they chose at the same moment to express in different language those rights which the agreement did not include, and which they never designed to part with, endeavoring thereby to prevent any cause for future altercation and *the intrusion into society of that doctrine of tacit implication which has been the favorite theme of every tyrant from the origin of all governments to the present day*.[14]

This language so aptly conveys the fears of many at the time—that the greatest threat of intrusion into individuals' personal lives was the government, and that it was viewed not primarily as an instrumentality to achieve ends, but rather this purpose was secondary and government's power a necessary evil to provide for certain other common goods, such as national defense and international trade.

In their well-known casebook *Administrative Law and Regulatory Policy*, U.S. Supreme Court Justice Stephen Breyer and Professors Stewart, Sunstein, Vermeule, and Herz provide a compelling overview of the development of the administrative state in the United States.[15] Their overview provides insight into the U.S. view as fearful of the state and placing greater trust in free markets to regulate activity rather than viewing the state as an instrument to limit the encroachment of individual freedoms by market actors. They divide this overview into temporal periods, which can be summarized in five transitions: (1) English antecedents and the American experience to 1875; (2) 1875–1930: the rise of regulation and the traditional model of administrative law; (3) the New Deal through 1965: the Administrative Procedure Act & the maturation of the traditional model of administrative law; (4) 1965–1985: critique and transformation of the administrative process; and (5) 1985–present: retreat or consolidation (the modern period).[16]

---

[12] *Id.* at 194.

[13] *Id.* at 196.

[14] *Id.* at 196–97 (emphasis added).

[15] STEPHEN G. BREYER ET AL., ADMINISTRATIVE LAW & REGULATORY POLICY 15–29 (7th ed. 2011).

[16] *Id.* at 15–29.

From the earliest days of the Republic until the present day, a consistent theme is present of reacting with hesitant and concern to expansion of the administrative state. In addition to the discussion above, Breyer's observations about the early periods highlight key quotes from The Federalist:

> In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself.[17]

> The accumulation of all powers, legislative, executive, and judiciary, in the same hands, whether of one, a few, or many, and whether hereditary, self appointed, or elective, may justly be pronounced the very definition of tyranny. . . . On the slightest view of the British Constitution, we must perceive that the legislative, executive, and judiciary departments are by no means totally separate and distinct from each other.[18]

These quotes, as with those discussed earlier, highlight the early fears the Framers had concerning state power. As the administrative state began to develop in the late 1800s and early 1900s, scholars differed as to whether it preserved or encroached upon the separation of powers viewed so necessary at the founding but generally viewed it with a cautious eye.[19] Even the effects of the Great Depression and World War II were insufficient to shift permanently the American skepticism of concentration of power. Congress begrudgingly hammered out the Administrative Procedure Act in the 1940s as a compromise designed to limit agency power in the wake of several wartime and post-Depression expansions of administrative power.[20] By the 1960s, 1970s, and 1980s, the trend had again swung fully toward limiting agency power as "[a]gencies were no longer viewed as clinicians,

---

[17] THE FEDERALIST NO. 51, at 294 (James Madison) (Am. Bar Ass'n ed. 2009).

[18] THE FEDERALIST NO. 47, at 271–72 (James Madison) (Am. Bar Ass'n ed. 2009).

[19] *See* Peter L. Strauss, *The Place of Agencies in Government: Separation of Powers and the Fourth Branch*, 84 COLUM. L. REV. 573, 609 (1984) (discussing the "general worrying about the relationship of the Presidency and administration" following the Civil War).

[20] *See* Administrative Procedure Act of 1946, Pub. L. No. 79–404 (codified as amended in scattered sections of 5 U.S.C.) (governing the way in which federal administrative agencies may propose and establish regulations); *see also* A.L.A. Schechter Poultry Corp. v. United States, 295 U.S. 495, 541–42 (1935) ("In view of the scope of that broad declaration, and of the nature of the few restrictions that are imposed, the discretion of the President in approving or prescribing codes, and thus enacting laws . . . is virtually unfettered. We think that the code-making authority thus conferred is an unconstitutional delegation of legislative power."); Panama Refining Co. v. Ryan, 293 U.S. 388, 432–33 (1935) (holding that the section of the National Industrial Recovery Act in question was an unconstitutional delegation of legislative power because it did not provide clear guidelines to the executive); J.W. Hampton, Jr. & Co. v. United States, 276 U.S. 394, 404–08 (1928) (holding that a congressional delegation of power under the Tariff Act was not unconstitutional).

and social policies were no longer viewed as amenable to correct solutions."[21] While social policy did advance at the legislative level during this period, agency skepticism remained, leading to substantial divisions between agencies and those they regulated.[22] Since the 1980s and through the present day, debate continues between formalists who believe in strict adherence to separation of powers out of fear of concentrated state power and functionalists who believe that some ground must be given to allow a complex society to function. In both cases, however, scholars, judges, and legislators recognize the dangers of concentration of power and view the administrative state with a cautious eye, at best accepting its power as a necessary evil. This differs substantially from the receptive European viewpoint where instrumentalist views of the role of the bureaucratic state and related European regulatory agencies receive more open welcome, particularly given the complexities of the modern, internet(worked) world.

Notwithstanding this view of the state, however, some concern with private action "bleeds over" from restraints on the State to restraints on private action. This is particularly true when the concern regarding harms flowing from state action involve the suppression of speech or expression. For example, in 1968 Congress passed and the President signed into law the Wiretap Act provisions of the Omnibus Crime Control and Safe Streets Act which amended 18 U.S.C. § 2511 to prohibit "*any person*" from "intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept [] any wire, oral, or electronic communication."[23] *Katz v. United States*[24] had overturned many years of telephone surveillance jurisprudence under *Olmstead v. United States*[25] and many years of public concern regarding surveillance activities by U.S. intelligence and law enforcement agencies as noted in the *Church Committee Report*.[26] As noted in the *Church Report*, "*Katz* explicitly left open the question . . . [of] whether or not a judicial warrant was required in

---

[21] Lisa Schultz Bressman, *Procedures as Politics in Administrative Law*, 107 COLUM. L. REV. 1749, 1761 (2007).

[22] *See* David Thaw, *Enlightened Regulatory Capture*, 89 WASH. L. REV. 329, 348–50 (2014) (providing examples of agency rulemaking failures resulting from the exclusion of some regulated parties in the rulemaking process).

[23] 18 U.S.C. § 2511(1) (2012) (emphasis added).

[24] 389 U.S. 347, 350–53 (1967) (holding that law enforcement use of an eavesdropping device to intercept the telephone conversation of a criminal suspect, without a judicial warrant, was an impermissible search under the Fourth Amendment).

[25] 277 U.S. 438, 466 (1928) (holding that the installation and use of a wiretapping device by law enforcement to monitor the telephone conversations of criminal suspects without first procuring a warrant did not amount to an unlawful search under the Fourth Amendment requiring suppression of the acquired evidence).

[26] *See* S. REP. NO. 94-755, at 670, 686 (1976) (discussing concerns of J. Edgar Hoover that the public would react adversely to learning of the FBI's "mail opening" technique).

cases 'involving the national security.'"[27]

In response to concerns regarding government surveillance, Congress included Title III (the "Wiretap Act") in the 1968 Omnibus Crime Control Act.[28] As noted by the Church Report, "the issue of 'national security' wiretaps, which was left open in *Katz*, was similarly avoided [in Title III]."[29] Interestingly, however, the Wiretap Act's breadth was not limited in scope to Government action. It specifically included "anyone" in its prohibition against wiretapping. This law, and many similar state analogs,[30] remains in effect today as a bulwark against suppression of expression by surveillance conducted both by the government and by private actors.

B. *Briefly about the Administrative State in the European Union and the regulation of data protection*

The European Union, by contrast, is not a real federalist state like the U.S. Quoting from a very important judgment of the European Court of Justice (ECJ):

> The [European] Community constitutes a new legal order of international law for the benefit of which the States have limited their sovereign rights, albeit within limited fields, and the subjects of which comprise not only member States but also their nationals. Independently of the legislation of member States, community law therefore not only imposes obligations on individuals but is also intended to confer upon them rights which become part of their legal heritage. These rights arise not only where they are expressly granted by the Treaty, but also by reason of obligations which the Treaty imposes in a clearly defined way upon individuals as well as upon the member States and upon the Institutions of the Community.[31]

It is not clear, in fact, what is "new" in the European Community, from a legal point of view.[32] According to some scholars, it can be viewed as a

---

[27] *Id.* at 288.

[28] *Id.*

[29] *Id*.

[30] *See Laws on Recording Conversations in All 50 States*, MATTHIESEN, WICKERT & LEHRER, S.C. (Jan. 19, 2017), https://www.mwl-law.com/wp-content/uploads/2013/03/LAWS-ON-RECORDING-CONVERSATIONS-CHART.pdf (stating which jurisdictions require getting consent of the person or persons being recorded).

[31] Case 26-62, N,V, Algemene Transport: en Expeditie Onderneming van Gend & Loos v. Netherlands Inland Revenue Administration (Feb. 1963) (Neth.) (reference for a preliminary ruling: Tariefcommissie).

[32] On these issues, see also Ugo Pagallo, La TUTELA DELLA PRIVACY NEGLI STATI UNITI D'AMERICA E IN EUROPA 111–113 (Giuffrè ed., 2008) (It.).

multi-level constitutional system,[33] for others it can be viewed as a sort of federalism à la European,[34] or a variation of the Medieval *jus commune*,[35] or a form of standard organization for the International Law.[36]

Besides the difficult classification of European federalism, it is interesting to note that the E.U. is a union of states and citizens with well-identified limits to the central authority. In fact, looking at E.U. legislative activity, member states are not inclined to welcome regulations which have immediate legal force for individuals within the member states, preferring instead the use of Directives, which need to be transposed in national laws to be fully effective in every single state.[37]

The difficulties of qualification of E.U. administrative state did not prevent the member states from striving for a common vision of privacy regulation among the states. This was clear since the beginning of Directive 95/46/EC, which defines a set of objectives that must be achieved by single state law and aims to create a common framework between the Member States.[38] After almost twenty years of existence of the Directive, the E.U. faced that the implementation of the objectives with single state law created "a fragmented legal environment which has created legal uncertainty and unequal protection for data subjects."[39] Thus in January 2012, the European Commission proposed a comprehensive reform of data protection rules, putting the completion of this reform as a policy priority.

The objective of this new set of rules is to return control of personal data to citizens, and to simplify the regulatory environment for businesses.

In fact, the data protection regulation is a pillar of the E.U. strategy for creating the so-called Digital Single Market, which aims to remove the barriers for Europeans when using online tools and services. The entire

---

[33] *See* Ingolf Pernice, *Multilevel Constitutionalism and the Treaty of Amsterdam: European Constitution-Making Revisited?*, 36 COMMON L. MARKET REV. 703, 707 (1999) (Neth.) (defining a multi-level constitution as a "constitution made up of the constitutions of the Member States bound together by a complementary constitutional body consisting of the European Treaties [].").

[34] *See* J.H.H. WEILER, THE CONSTITUTION OF EUROPE: "DO THE NEW CLOTHES HAVE AN EMPEROR?" AND OTHER ESSAYS ON EUROPEAN INTEGRATION 24 (Cambridge Univ. Press ed., 1999) (describing the constitutional system among the European Community).

[35] *See* H. Coing, *Von Bologna bis Brussels: Europäische Gemeinsamkeit, Gegenwart und Zukunft*, Kölner Juristische Gesellschaft, IX, Bergish Gladbach-Köln, 1989.

[36] *See* Theodor Schilling, *The Autonomy of the Community Legal Order: An Analysis of Possible Foundations*, 37 HARV. INT'L. L.J. 389, 396–97 (1996) (discussing how the case law of the ECJ shows an evolution and adoption of treaties as a constitution).

[37] *See* Daniel Halberstam, *Comparative Federalism and the Issue of Commandeering*, *in* THE FEDERAL VISION: LEGITIMACY AND LEVELS OF GOVERNANCE IN THE UNITED STATES AND THE EUROPEAN Union 214 (Kalypso Nicolaidis & Robert Howse eds., 2001) (explaining how member states pass Directives which require legislative action to become fully effective within that state).

[38] *See* Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERKELEY TECH. L.J. 461, 467–469 (2000).

[39] Viviane Reding, *The European Data Protection Framework for the Twenty-First Century*, 2 INT'L DATA PRIVACY L. 119, 121 (2012).

strategy is focused on creating an area of trading which could contribute €415 billion to the European economy, boosting jobs, growth, competition, investment and innovation.

Thus, there are strong economic basis behind this reform, which is composed of two legal texts: the General Data Protection Regulation (GDPR)[40] and the Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.[41]

The GDPR will be applicable starting in May 2018 and will have a tremendous impact on data protection regulation.

Another step of the Digital Single Market strategy is about cybersecurity, which is often connected with data protection issues. In this sense, the Network Information Security Directive, as stated by the European Commission, will provide legal measures to boost the overall level of cybersecurity in the E.U. by ensuring:

- Member States preparedness by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority;
- cooperation among all the Member States, by setting up a cooperation group, in order to support and facilitate strategic cooperation and the exchange of information among member states. They will also need to set a CSIRT Network, in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks;
- a culture of security across sectors which are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare, and digital infrastructure. Businesses in these sectors that are identified by the member states as operators of essential services will have to take appropriate security measures and to notify serious incidents to

[40] *See* Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016 O.J. (L. 119/1) (explaining that one example is the recent decision to remove roaming costs by 2017 between the European mobile phone operators).

[41] Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/911/JHA, 2016 O.J. (L. 119/89).

> the relevant national authority. Also key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive.[42]

In a message from July 5, 2016, the European Commission "encouraged Member States to make the most of NIS coordination mechanisms" and signed an agreement with members of the cybersecurity industry to better equip Europe against cyber-attacks and to strengthen the competitiveness of its cybersecurity sector—creating a contractual Public-Private Partnership (cPPP)—which is expected to drive further market-oriented policy measures in the forthcoming months.[43]

II. DEFINING THE IDEA (NOT THE LAW) OF PRIVACY FOR U.S. AND E.U. CITIZENS: SIMILITUDES AND DIFFERENCES

This Section builds on the comparative analysis of the administrative state in the U.S. and E.U., translating those differences into a framework for understanding the origins of privacy regulation in each society and investigating what commonalities might exist. Using a perhaps-controversial approach to define privacy not starting from the premise of *existing law*, but rather from the premise of what are the underlying historical concerns, it proceeds to identify that the two respective privacy regulatory frameworks share a common fear of privacy invasions as "chilling," or deterring, certain actions by individuals. The frameworks diverge, however, with respect to with which *actors* each society seems most concerned will engage in such invasion.[44] Following from the discussion in Section I, this Section argues that U.S. privacy regulation focuses on chilling effects of state action, whereas E.U. privacy regulation focuses on chilling effects of (private) corporate action.

A. *The Concept of "Chilling Effects"*

"Chilling Effects" is a much celebrated concept in jurisprudence and scholarship in the United States, especially related to the First Amendment.[45] It describes a condition in which invasions of privacy or the fear thereof

---

[42] *The Directive on Security of Network and Information Systems (NIS Directive)*, EUR.COMMISSION (July 28, 2016), https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

[43] *Id*.

[44] It is worth nothing that multiple scholars have observed that the U.S. and E.U. perceptions of privacy also diverge in their concept of privacy as an "exclusionary" versus a "fundamental" right, and in the degree to which that right is a political decision or a Constitutionally-binding choice. Such distinctions, while quite important, are orthogonal to the argument of this Section, which focuses on the historical similarities of "fear against invasion" inherent in both societies' views of privacy.

[45] *See* Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the "Chilling Effect"*, 58 B.U.L. REV. 685 (1978).

cause individuals to change their behaviors, abstaining from otherwise-lawful activity not because of its proscription by society but out of fear of public association with that activity. This concept is a value shared by many societies around the world and provides a starting point from which to identify more specific normative values regarding privacy shared among U.S. and E.U. nations.

The concept of "Chilling Effects" is defined by two characteristics: (1) that individuals perceive there is at least a risk of their activity or condition being observed by another who may disseminate those observations; and (2) that individuals change their behavior—discontinuing or hiding that activity or condition—out of fear of public association with that activity or condition.[46] This formulation suggests a means of identifying shared intrinsic privacy commitments among nations whose extrinsic (expressed through law) privacy commitments may differ widely.

Historically, the U.S. Supreme Court has been reluctant to recognize chilling effects as a sufficient ground for a violation of constitutional rights,[47] while in the E.U. the European Court of Human Rights, the European Court of Justice and many state courts have recognized many times that the possibility of undisclosed collection and storage of personal identifiable information can create a danger for fundamental rights,[48] but despite this, the E.U. courts have been in general reluctant to recognize chilling effects when people give their consent to data processing.

A recent study, however, has shown that there is a risk that people will experience a chilling effect when consenting to the disclosure of personal identifiable information, intending the chilling effect "as an increased propensity to comply with social norms."[49] Both the increase in societal

---

[46] *See* Brief of *Amici Curiae* First Amendment Legal Scholars, *Wikimedia Foundation v. Nat'l Security Agency*, 143 F. Supp. 3d 344 (D. Md. Dec. 18, 2015) at 3, 8–9, http://www.margotkaminski.com/wp-content/uploads/2015/09/085-001-Brief-of-Amici-Curiae-First-Amendment-Legal-Scholars-1.pdf; *see also id.* at 362 n.27 (recognizing the importance of "chilling" but rejecting that as adequate to establish standing); *see also generally* Clapper v. Amnesty Int'l, 568 U.S. 398 (2013); McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995); Laird v. Tatum, 408 U.S. 1 (1972).

[47] *See*, *e.g.*, Clapper, 568 U.S. at 418 (noting the plaintiffs could not establish standing by claiming they experienced a chilling effect that resulted from a governmental policy); Laird, 408 U.S. at 3 (rejecting the complaint of a "'chilling effect' on the exercise of the First Amendment rights where [the] effect is [] caused . . . only [by] the existence . . . of intelligence gathering").

[48] *See*, *e.g.*, Tele2 Sverige AB v. Post-och telestyrelsen and Sec. of State for the Home Dep't. v. Tom Watson et al., Joined Cases 203/15 and 698/15 ECJ (2016) (emphasizing the importance of protection of the right to privacy and confidentiality with respect to the processing of personal data) and Bărbulescu v. Romania, application no. 61496/08 ECtHR (2017) (emphasizing that communications in the workplace are covered by the concepts of "private life" and "correspondence" protected by Article 8 of the European Convention of Human Rights).

[49] *See* Yoan Hermstrüwer & Stephan Dickert, *Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten* 3 (Preprints of the Max Planck Institute for Research on Collective Goods, Working Paper No. 5, 2013).

recognition of chilling effects and the acknowledgement (if not doctrinal acceptance) by high courts in both the U.S. and E.U. suggest that, from a political compatibility standpoint, the two societies share concern for the implications of chilling effects. The shared historical antecedents of "feared invasion" into (private) seclusion, discussed in more detail in Section I, suggest that adequate shared privacy commitments exist across the Atlantic to examine harmonization efforts on that basis.[50]

Identifying shared intrinsic privacy commitments, therefore, lends weight to two essential arguments of this Article: (1) that procedural harmonization is a plausible goal; and (2) that trusting the market—through delegation of compliance details to regulated entities—is reasonable given these shared commitments.

B. *Overview of U.S. Privacy Regulation*

This subsection provides an overview of Constitutional, statutory, and other privacy protections in the United States. The next subsection similarly overviews parallel protections in the European Union. Subsection D then compares these two regimes to demonstrate the plausibility of procedural harmonization.

1. *Constitutional Protections*

There is no express privacy right in the U.S. Constitution. Rather, there are effective rights that derive, either directly or indirectly, from the protections afforded by the Amendments in the Bill of Rights. Direct derivative rights are those which necessarily flow from the express provisions of the Bill of Rights. For example, a privacy interest in one's person, residence, and certain other excludable property flows from the Fourth Amendment.[51] Indirect derivative rights are those the courts have recognized as necessary corollaries to the privileges afforded by the Bill of Rights Amendments. A privacy interest in one's associative activities, for example, has been recognized in certain contexts as flowing from the First (and Fourteenth) Amendments.[52] A general privacy interest in the "marital bedroom" has been recognized as flowing indirectly from a collection of

---

[50] *See supra* Section I.

[51] *See* Schmerber v. California, 384 U.S. 757, 767 (1966) ("The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State"); Priscilla J. Smith et al., *When Machines Are Watching: How Warrantless Use of GPS Surveillance Technology Violates the Fourth Amendment Right Against Unreasonable Searches*, 121 YALE L.J. 177, 183–84 (2011) (discussing Kyllo v. U.S., 533 U.S. 27 (2001)).

[52] *See*, *e.g.*, NAACP v. Alabama, 357 U.S. 449, 466 (1958) (stating that there is immunity from state scrutiny of membership lists under the First and Fourteenth Amendments, applying the First Amendment protections to "associate freely with others" to action by individual states under the Fourteenth Amendment and holding that Alabama failed to demonstrate a "controlling justification for the deterrent effect on the free enjoyment of the right to associate").

several of the Bill of Rights Amendments.[53]

These provisions share all concern restraints on government action, as opposed to a general privacy interest. At a general level, however, they implement three substantive privacy commitments (if only against certain actors): (1) a privacy interest in residential (and similar) spaces; (2) a privacy interest in one's own body; and (3) a privacy interest in state-recognized marital relationships.

2. *Federal Statutory Protections Concerning Government Processing of Information (the Privacy Act of 1974)*

The Privacy Act of 1974 places obligations on most elements of the U.S. federal government which process information records describing individuals.[54] It limits the government from disclosing information from systems of records absent express consent of the individual or if the disclosure falls into one of a list of enumerated statutory exceptions. It is the only (non-sector specific) privacy law of general applicability imposing affirmative duties on a data processor in the United States, but is limited solely to (federal) government actors. On a general level, the Privacy Act implements a substantive commitment to the privacy of non-public individuals' information acquired by government systems, but only as it pertains to the federal government as a data processor and subject to several exceptions. Additionally, the Privacy Act only applies to government agencies, and not to the courts, legislature, or non-agency executive entities. The Act thus provides limited input describing potential shared substantive privacy commitments, however it does indicate a receptiveness in the United States to the concept of a general information processing privacy law as pertained the "feared actor" (the state) in the United States.

3. *Federal Sector-Specific Statutory Provisions*

Many industries are subject to sector-specific regulation in the United States, but two stand out prominently in the privacy context. Both the healthcare and finance industries have comprehensive legislation requiring both specific actions by regulated entities and requiring those entities to develop (and adhere to) compliance plans for managing substantive privacy commitments and the information security measures that implement those commitments. Financial entities are covered by the Gramm-Leach-Bliley Act (GLBA)[55] and healthcare entities are covered by the Health Insurance

---

[53] *See*, *e.g.*, Griswold v. Connecticut, 381 U.S. 479, 486 (1965) (asserting that marriage is a "right of privacy older than the Bill of Rights").

[54] Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a) (summarizing when the privacy of an individual is directly affected).

[55] Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. §§ 6804, 6805 (2012).

Portability and Accountability Act (HIPAA).[56] Notably, as Thaw describes elsewhere, both these statutory frameworks utilize a form of Management-Based Regulatory Delegation.[57]

These two statutory frameworks—both of which apply to private actors—implement general substantive commitments to privacy in two specific information areas: (1) medical/healthcare information; and (2) personal financial information.

4. *Federal Medium-Specific Statutory Provisions*

In additional to affording protections for information in specific substantive areas, such as that processed by healthcare and financial industries, U.S. federal law (and some U.S. states) afford statutory protections to information conveyed via certain media. For example, mail sent via the U.S. Postal Service is subject to statutory protection prohibiting its interception (or surveillance) both by private and government actors (with limited exceptions)."[58] Likewise, the Wiretap Act provides similar protections against the interception of telephone, telegraph, and similar communications.[59] Amendments to the Wiretap Act included in the Electronic Communications Privacy Act (ECPA) provide similar protections for computer and information system based data communications via telecommunications systems while in-transit,[60] and amendments to the Wiretap Act included in the Stored Communications Act (SCA) provided similar protections (of limited temporal duration) for such data while at rest.[61]

This statutory framework—which, subject to various exceptions, applies both to state and to private actors—implements a general substantive commitment to the privacy of information being processed for transit (and in some cases storage) by telecommunications networks.[62]

5. *Federal Consumer Protection Law and the FTC*

The Federal Trade Commission Act makes unlawful unfair and deceptive trade practices and grants the Federal Trade Commission the

---

[56] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18 U.S.C., 26 U.S.C., 29 U.S.C., and 42 U.S.C.).

[57] *See* David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U.L. REV. 287, 314–17, 324–36 (2014) (comparing the efficacy, in the cybersecurity context, of "[m]anagement-[b]ased [r]egulatory [d]elegation" to other types of regulation such as "[d]irective [r]egulation").

[58] S*ee* 18 U.S.C. § 1701, 1708.

[59] 18 U.S.C. § 2511 (2008).

[60] H.R. 4952, 99th Cong. (1986).

[61] *See id.* (including the subtitled Stored Communications Act (codified as amended at 18 U.S.C. § 2701)).

[62] Note, however, that this commitment does not extend to actors who provide the endpoint equipment, such as a computer provided by an employer or a wireless network provided by an educational institution.

authority to bring adjudicatory enforcement procedures against entities who engage in such practices.[63] The FTC has used this authority to engage in a substantial amount of privacy-related regulatory activities for nearly two decades.[64] The FTC's scope of enforcement authority is broad with respect to both the industrial sector and the nature of data or technology, but its regulatory activities are primarily reactive.[65] Furthermore, the FTC's participation in regulating privacy and data security activities was a self-granted power inasmuch as the FTC Act does not in any way expressly address that authority.[66] Other limited authority has, however, been granted to the FTC by Congress in this regard, such as the regulation of data collection regarding the online activities of children.[67]

It is difficult to draw conclusions regarding what substantive privacy commitments, if any, the FTC Act and the FTC's privacy and data security jurisprudence implement. At best, a commitment to preventing deception regarding privacy practices can be inferred from the Act and the Commission's enforcement activities. A broad reading of the scope of the Commission's enforcement activity might suggest a commitment to "reasonable" privacy and security practices, but this topic is subject to substantial debate[68] and there is insufficient evidence to conclude it implements a clear substantive privacy commitment.

6. *State Statutory Privacy Privileges*

Most U.S. jurisdictions afford special privileges to certain types of communications between specific parties. These privileges can take the form of evidentiary privileges (preclusions of the introduction of such communications during formal adjudicatory or judicial proceedings) and/or confidentiality requirements on the part of certain parties. The most common examples include communications with attorneys, psychotherapists (as separate from other medical practitioners), medical practitioners (to a lesser degree), and clergy. In most U.S. jurisdictions, these parties both are required to keep confidential certain information acquired in their professional capacity and the government is precluded (in most circumstances) from attempting to acquire that information from the

---

[63] 15 U.S.C. § 45(a)(1) (2006).

[64] *See generally* Chris Jay Hoofnagle, FEDERAL TRADE COMMISSION LAW AND POLICY (2016).

[65] Thaw, *The Efficacy of Cybersecurity Regulation*, *supra* note 57, at 336–40; *see also* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014); David Bernard Thaw, Characterizing, Classifying, and Understanding Information Security Laws and Regulations: Considerations for Policymakers and Organizations Protecting Sensitive Information Assets (Ph.D. Dissertation, University of California, Berkeley) (May 11, 2011, on file with the University of California), http://www.davidthaw.com/papers/DavidThawDissertationFinal.pdf ("Unlike the assessments conceived under traditional management based regulation, FTC-ordered assessments are reactive in nature instead of proactive.").

[66] *See* Solove & Hartzog, *supra* note 65, at 598–99.

[67] 15 U.S.C. § 6502(b) (1998).

[68] FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 246 (3d Cir. 2015).

professional or the individuals they serve. Additionally, while no duty of confidentiality exists between spouses, the government is prevented from compelling spouses to disclose information about one another in criminal matters.

These examples again implement the substantive privacy commitment to the protection of healthcare and medical information and to the protection of marital intimacy. Additionally, they describe several other examples, such as legal advice and spiritual advice, where U.S. law recognizes certain substantive privacy commitments.

7. *State Security Breach Notification Laws*

Nearly all U.S. jurisdictions have security breach notification (SBN) laws which require the custodian of sensitive data or data processor to notify individuals described in data that custodian holds or processes in the event this sensitive data becomes compromised by an unauthorized party. The implementation of these laws varies from jurisdiction-to-jurisdiction, but they all implement an underlying substantive privacy commitment that individuals are entitled to be informed when certain sensitive data may have been accessed and/or acquired by an unauthorized party.

C. *Overview of E.U. Privacy Regulation*

This section provides an overview of E.U. privacy protections parallel to that in section B.

1. *Constitutional Protections*

The starting point of privacy protection from a constitutional point of view is Article 7 of the Charter of Fundamental Rights of the European Union,[69] which states the right of respect for private and family life,[70] and Article 8 regarding the protection of personal data.[71] They are both positive rights, and they are identified, unlike in the U.S. Constitution, as fundamental rights.

Looking at the time when the Charter was issued, however, it is evident that it comes after many years of privacy legislation in the E.U., both in

---

[69] Charter of Fundamental Rights of the European Union art. 7 2010 O.J. C 83/02, http://fra.europa.eu/en/charterpedia/article/7-respect-private-and-family-life.

[70] *Id.* ("Everyone has the right to respect for his or her private and family life, home and communications.").

[71] Charter of Fundamental Rights of the European Union art. 8 2010 O.J. C 83/02, http://fra.europa.eu/en/charterpedia/article/8-protection-personal-data ("1. Everyone has the right to the protection of personal data concerning him or her . . . . 2. Such data must 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. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified . . . . 3. Compliance with these rules shall be subject to control by an independent authority.").

member states—for example France, Denmark, Sweden or Germany—and in the European community, with Directive 95/46/EC.

To look at an older source of law, Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedom was signed in Rome in 1950, and it establishes the right of respect for private and family life.[72] It is interesting to note that, for the first time, the E.U. has a rule against unreasonable invasion of privacy "by a public authority" akin to those found in the United States. Finally, the importance of this rule is underlined in Article 6, Section 3, of the Treaty on European Union.[73]

Another issue that must be considered regarding the constitutional protections of privacy in the E.U. is that the rules just cited do not overwrite the basic rules provided, for example, by the constitutions of the single member states. This creates a legal patchwork that needs harmonization[74] and implies the use of the directives and subsequent transposition by member states.

2. *Federal Statutory Protections Concerning Processing of Information*

The most important law, excluding the soon to be enforced General Data Protection Regulation (GDPR),[75] is Directive 95/46/EC, enacted in 1995.[76] The aim of the Directive is to harmonize the privacy regulations in all member states by setting out common rules for data protection.

The first effort was to identify, in Article 2, a set of definitions as

---

[72] *See* Charter of Fundamental Rights of the European Union art. 7 2010 O.J. C 83/02, *supra* note 69 ("1. Everyone has the right to respect for his private and family life, his home and his correspondence. . . . 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.").

[73] *See* Treaty on European Union (consolidated version) No. 6655/1/08 REV 1 of Apr. 30, 2008, art. 6 § 3, http://www.europarl.europa.eu/hearings/20000222/libe/art6/default_en.htm ("Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law.").

[74] *See* D. J. SOLOVE & P. M. SCHWARTZ, INFORMATION PRIVACY LAW 1110 (Aspen ed. 2011) ("This term of European community law refers to formal regulatory attempts to increase the similarity of legal measures in member states.").

[75] Regulation (EU) 2016/679 of the European Parliament & of the Council of 27 April 2016 http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=IT.

[76] Directive 95/46, of the European Parliament and of the Council of 24 October 1995 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).

"personal data,"[77] "processing of personal data,"[78] "controller,"[79] "processor,"[80] and "data subject's consent."[81] Thus, we may now find a set of definitions in all privacy laws of member states, even if this set is not exactly the same of the Directive.

Another important rule is Article 5, regarding the implementation of the Directive by member states,[82] which provides general parameters for the transposition of the Directive's provisions by each member state. It is important because it is another example of the refusal of direct regulation from central authority.

The Directive includes every possible processing of data, with some exception for public security, state security, and criminal law. One of the most important requirements set by the Directive is the duty, for the data controller, to preliminary inform the data subject on the purposes for which the data are intended. After the information, with some exceptions, the data subject must express his or her consent to data processing, especially for data used for direct marketing or profiling of customers. The data subject also has a permanent right to monitor and challenge the use of his or her personal data for all the steps of processing until the lawful destruction of data themselves.

The Directive, finally, prescribes the creation of a Data Protection Authority in every member state to supervise the enforcement of the Directive and of the national privacy regulation.

The General Data Protection Regulation (GDPR) (effective May 2018) represents an important change from the nature of previous legal tools used: while a "Directive" aims to set common objectives and leave to each of the

---

[77] *See id.* at 8 ("'[P]ersonal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity[.]").

[78] *See id.* ("'[P]rocessing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction[.]").

[79] *See id.* ("'[C]ontroller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law[.]").

[80] *See id.* ("'[P]rocessor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller[.]").

[81] *See id.* at 9 ("'[T]he data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.").

[82] *See id.* ("Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.").

Member States the form and the method by which the Directive is transposed into national law, by contrast a "Regulation" is binding in the form is issued. This means that the Regulation is much less "elastic" in its implementation than would be a Directive.

Thanks to the GDPR, "[c]onsistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union,"[83] but the GDPR itself leaves some margin of discretion to the Member States for some specific situations (e.g. for the processing of sensitive data).

The GDPR, then, is a comprehensive legal text that leaves some limited topics to be defined by the single states. The domestic Data Protection Authorities, a supranational organization like the Article 29 Working Party, or the European Data Protection Supervisor may assist in this process.

In this regard, the ICO issued a guide[84] on March 17, 2017 for migrating to the new General Data Protection Regulation, and the Article 29 Working Party is publishing several guidelines to help promulgate understanding of the new or different obligations included into the GDPR.[85]

3. *Federal Medium-Specific Statutory Provisions*

A good example of the Federal Medium-Specific Statutory Provision is Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Commission Regulation (E.U.) No. 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC. It provides a basic rule for the so-called "unsolicited communications" by automated telephone calls, faxes, texts and e-mail, which is the "opt-in" rule. According to Article 13, the data subjects need to express his or her consent to receive commercial communications regarding goods or services offered by a company, and they have a permanent right to "opt-out" and stop the delivering of these communications.

The text of the Directive was amended by Directive 2009/136/EC and now includes the definition of personal data breach, which means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available

---

[83] Regulation 2016/679, *supra* note 40, at n.10.

[84] Information Commissioner's Office, *Preparing for the General Data Protection Regulation: 12 Steps to Take Now* (May 2017), https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf.

[85] For example, the Article 29 Working Party has already issued guidelines on the right to data portability, on the designation of a data protection officer and on how to identify a controller or processor's lead supervisory authority. Article 29 Working Party, EUROPEAN COMMISSION, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

electronic communications service in the Community."[86]

This Directive, called the ePrivacy Directive, is now undergoing a reformation process likely to result in a new version sometime in late 2017 or early 2018.[87]

4. *State Statutory Privacy Privileges: The Italy Case*

The member states have usually transposed the principles of Directives 95/46/EC and 2002/58/EC with satisfactory compliance. In some cases, however, states have extended the principles of the Directives by adding other rules for data processing.

In Italy, for example, the failure to adopt the minimum security measures[88] in data processing is a criminal offense, which can be punished by detention for up to two years.

Italy has also implemented the steps to be taken following a personal data breach.[89] These steps include notifying the Italian Data Protection Authority without undue delay and, if the personal data breach is likely to be detrimental to the personal data or privacy of the contracting party or another individual, the provider must also notify without delay the breach to the contracting party or the individual.[90]

In addition, the notification to the contracting party or individual must at least include a description of the nature of the personal data breach and the contact point where additional information can be obtained, and it must list the measures recommended to mitigate the possible detrimental effects of the personal data breach.[91] The Italian Data Protection Authority, from its side, may issue a decision containing guidelines and instructions with regard to the circumstances under which a provider is obliged to notify personal data breaches, the format of such notification, and the manner in which the notification is to be made.[92]

---

[86] Directive 2009/136, of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws, 2009 O.J. (L 337) 29.

[87] On January 10, 2017 the draft text "Proposal for a Regulation on Privacy and Electronic Communications" was issued. *Proposal for a Regulation on Privacy and Electronic Communications*, EUROPEAN COMMISSION, https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

[88] Legislative Decree no. 196 of 30 June 2003 (defining misuses in Section 33 of the Legislative Decree n.196 of 30 June 2003 as "the minimum security measures . . . in order to ensure a minimum level of personal data protection.").

[89] *See id.* (showing Italy's implementation of an entire data protection code).

[90] *See id.* (requiring the provider of a publicly available communications service to inform subscribers and, if possible, users about the risk of network security breach).

[91] *Id.* (requiring the provider to also report it to the government's security data authority).

[92] Section 32 of Legislative Decree no. 196 of 30 June 2003.

D. *U.S. – E.U. Shared Commitments*

As discussed in the preceding sections, U.S. and E.U. privacy law have many textual and structural differences. We begin with a comparative examination summarizing these differences, and then shift to discuss commonalities, how those commonalities suggest the plausibility of procedural harmonization, and how such harmonization is possible notwithstanding these differences.

Unlike the European Union, privacy law in the United States lacks a central, unifying framework. There is no general privacy law in the United States, which comprises rather a patchwork of constitutional, statutory, and regulatory mechanisms, each giving effect to different privacy protections. Many of these protections are incidental to other rights.[93] The most prevalent elements of this patchwork includes constitutional protections (express and implied), federal statutory protections concerning government processing of information, federal statutory protections concerning sector-specific or communications-medium specific processing of or access to information, federal regulatory interpretation of general consumer protection statutes, and state statutory (evidentiary and other) privacy privileges and breach notification obligations.[94]

Most notably, these protections nearly all take the form of negative liberties—rights precluding a specific actor from taking a specific action. This starkly contrasts with the E.U. approach, which, as discussed below, adopts a positive liberties approach including enumerated rights. This section briefly outlines the protections described above and extrapolates from those protections a set of common "core commitments" present in U.S. privacy protections.[95]

As noted by James Q. Whitman, "we are in the midst of significant privacy conflicts between the United States and the countries of Western Europe—conflicts that reflect unmistakable differences in sensibilities about what ought to be kept 'private.'"[96]

In fact, there are different privacy habits between the U.S. and E.U. For example, discussion of salary and compensation is permitted in the U.S., while many E.U. countries frown upon or prohibit disclosure of this information. Aside from different habits, however, E.U. privacy regulation is generally more protective for certain kinds of privacy like consumer data, credit reporting, employees in the workplace, discovery in civil litigation,

---

[93] *See*, *e.g.*, Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (describing the concept of "penumbras" giving rise to privacy rights inherent in the First, Third, Fourth, and Fifth Amendments to the U.S. Constitution).

[94] *See* McGeveran, *supra* note 2, at 972–79.

[95] *See id.*

[96] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1155 (2004).

dissemination of images of minors, and cameras used in public areas. Some of these protections, particularly employee and litigation privacy, may strike Americans as unusual. They are, however, commonplace for for Europeans and likely well-depict the nature of the U.S.-E.U. substantive privacy conflict. This conflict has led to many disputes, in particular trade-related battles, stemming in non-trivial part from these different privacy perceptions.[97]

One of the paramount cases about the different view of privacy is the controversial ECJ's decision of the "right to be forgotten."[98] While some U.S. privacy scholars are stating that "[t]his is a form of censorship, one that would most likely be unconstitutional if attempted in the United States,"[99] E.U. privacy scholars are more optimistic because

> the positive aspect of this decision is that it induces to reconsider positively the Article 17 of the EU Proposal for a General Data Protection Regulation, which is clearer that the scenario depicted by this decision. This provision admits a specific exception for freedom of expression and recognizes the role played by courts and regulatory authorities in deciding which data must be erased. Finally, it empowers the Commission to define detailed procedures and solutions to delete personal information.[100]

The contrast between these two conceptions of privacy, as noted by Robert Post, describes a great difference: continental privacy protection is a form of protection of personal dignity, American privacy protection is a form of protection of personal liberty.[101]

Starting from this difference, it is easy to understand why U.S. citizens are more concerned about privacy invasion by the state, especially within

---

[97] *See*, *e.g.*, Case C-317/04 & C-318/04, Parliament v. Council & Parliament v. Comm'n, 2015 E.C.J. I-4755 (holding that the arrangements on the transfer of Passenger Name Records of air passengers from the E.C. to the US Bureau of Customs and Border Protection were illegal and should be annulled).

[98] Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, 2013, ¶ 102.

[99] Jonathan Zittrain, *Don't Force Google to 'Forget'*, N.Y. TIMES, May 14, 2014, at A29; *see also* Daniel Solove, *What Google Must Forget: The EU Ruling on the Right to Be Forgotten*, LINKEDIN (May 13, 2014), https://www.linkedin.com/pulse/20140513230300-2259773-what-google-must-forget-the-eu-ruling-on-the-right-to-be-forgotten?trk=object-title [] ("[A]lthough recognized in US law, the right to be forgotten only exists in a few pockets of the law and is nothing compared to the rather dramatic ruling of the EU Court.").

[100] Alessandro Mantelero, *A Few Notes About the Google Case and the Right to Be Forgotten*, ICT L. & DATA PROT. (May 14, 2014), https://ictlawandataprotection.wordpress.com/2014/05/14/a-few-notes-about-the-google-case-and-the-right-to-be-forgotten/.

[101] *See* Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2087–95 (2001) (describing "different and in some respects incompatible concepts of privacy").

the "sanctity" of their own homes,[102] and E.U. citizens are more concerned about privacy invasion from the media or corporations.[103] It is easy to understand, similarly, why American privacy law framework is made by many statutory provisions containing negative rights, as seen in Section II, and continental privacy framework is more systematically developed focusing on positive rights.

Notwithstanding these differences, however, this Article advances the proposition that shared fears of "privacy invasion"—beginning from the concept of Chilling Effects—make procedural regulatory harmonization between U.S. and E.U. regimes possible. As noted by Professor Whitman,[104] for example:

> [I]t would be wrong to say that there is some absolute difference between American and continental European law. But the issue is not whether there is an absolute difference. . . . [I]t is the relative differences that matter. Americans and Europeans certainly do sometimes arrive at the same conclusions. Nevertheless, they have different starting points and different ultimate understandings of what counts as a just society.

This little excerpt exemplifies this Article and similar others, because despite the differences we have enumerated above, there are common fears that can form the foundation of common privacy regulation between the two western blocs.[105] This common foundation can make such regulatory harmonization usable, effective, and enforceable by the constituent nations and states. Reaching a unified privacy regulation represents a good opportunity for free exchange of personal identifiable information, with advantages for trading and in general free circulation of people and goods.

Even if the perceptions of privacy views are different, U.S. and E.U. have shared commitments about data protection and data processing. We can find a form of convergence if we look at the General Data Protection

---

[102] Boyd v. United States, 116 U.S. 616, 630 (1886); *see* Solove, *supra* note 99 (reporting on the E.U. Court's decision to protection citizen's privacy from being stored permanently).

[103] *See* Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315 (2000).

[104] Whitman, *supra* note 96, at 1163.

[105] *See* GABRIELA ZANFIR, EU AND US DATA PROTECTION REFORMS: A COMPARATIVE VIEW 217–22 (2012) (providing a comparative view of data protection reform projects from the U.S. and the E.U.); DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 1–3 (2013); Kenneth Bamberger & Deirdre Mulligan*, Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 247–54 (2011) (reporting findings from studies of corporate privacy managers); Francesca Bignami, *European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C.L. REV. 609, 682–683 (2007). Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 U. OTTAWA L. & TECH. J. 357, 357–60 (2005) (suggesting, as a compromise, the Canadian approach to privacy and personal information regulation).

Regulation (GDPR) and specific U.S. law such as the Consumer Privacy Bill of Rights. Some differences still exist,[106] but both approaches would provide accountable and effective safeguards for individuals and consumers against the rapid evolution of technology, surveillance, profiling techniques, and both reforms look forward to "a more protected individual [and consumer] and a more responsible data controller or data processor."[107] While not formally codified into U.S. law, this comparative example lends support to the proposition that certain common goals underlie both U.S. and E.U. privacy regulation.

Yes, differences in privacy regulation between the U.S. and E.U. will likely remain. This is why we believe that the answer to a unified privacy regulation cannot derive from convergence of existing laws but rather requires a new, bottom-up approach, using Management-Based Regulatory Delegation (or "Federated Regulation") theory applied to federalist systems of governance. We call this application Market-Supervised Regulatory Delegation.

III. COMMON GROUND IN U.S. AND E.U. BUREAUCRATIC ORGANIZATION: UNIFYING PRIVACY REGULATION—"MARKET-SUPERVISED REGULATORY DELEGATION"

Market-Supervised Regulatory Delegation presents a theoretical framework in which nation-parties to a multi-lateral agreement consent to limited general principles and a common enforcement procedure, and then implement those principles into law—while each still retains substantial ability to implement their own national policy choices. Private actors are free to choose in which nations to conduct business,[108] but that choice is no longer dominated by the transaction cost of varying regulatory compliance

---

[106] The main difference is the broad scope of the Regulation compared with the narrow scope of the CPBR.

[107] ZANFIR, *supra* note 105, at 217, 222.

[108] This method also is superior to current policy in that current (and recent) policy frameworks, such as the former U.S.-E.U. Safe Harbor and the new U.S.-E.U. Privacy Shield fail to give effect to respective nations' privacy protections. In practice, these agreements merely require data processors established in the U.S. to certify that they comply with the Principles defined to meet the E.U. data protection safeguards. *See Requirements of Participation*, PRIVACY SHIELD PROGRAM, https://www.privacyshield.gov/article?id=Requirements-of-Participation (last visited Mar. 1, 2017) (requiring public commitment by corporation to abide by the Privacy Shield Principles). Clever names notwithstanding, these agreements do not effectively extend E.U. member states' protections to the processing of data of E.U. citizens within the United States for companies participating in the Privacy Shield. Some criticisms in that sense were expressed by the Article 29 Working Party. *See* Statement, Article 29 Working Party, Statement on the Decision of the European Commission on the EU-US Privacy Shield (July 26, 2016), http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf ("It also remains unclear how the Privacy Shield Principles shall apply to processors.").

procedures.[109] Rather, the dominant factor in the choices by market participants to conduct business in a given nature is the *substantive* policy choices of that nation. This allows the market to express global preferences without intruding on the sovereign power of nations to make local policy decisions (albeit informed by—and perhaps even pressured by—such global market forces).

This Section builds upon the work in Sections I and II to propose a method for unifying the *process* of administering U.S. and E.U. privacy regulation by applying concepts of Federated Regulation (Management-Based Regulatory Delegation) theory to cross-jurisdictional privacy management. Such an approach establishes a regime under which aspirational goals are laid out by the legislative bodies (i.e., protection against "chilling effects" through a list of enumerated positive privacy "rights"), which then require the individual jurisdictions to prescribe (through their respective administrative processes) that regulated entities develop compliance plans to achieve these aspirational goals. By standardizing the compliance process, transaction costs for multi-national organizations to operate in multiple jurisdictions are lowered. While various jurisdictions may require more stringent privacy protections, the standardized compliance process facilities organizations' ability to make market-based choices regarding the jurisdictions in which to operate.

The result becomes a system under which each sovereign nation retains the ability to select those privacy norms they wish to enforce, and leaves more to market function the choices both of consumers and multi-national organizations the jurisdictions in which they wish to operate. This is accomplished by the application of a form of process-based standards regulation known as Federated Regulation (a form of Management-Based Regulatory Delegation). When applied across nations, we describe this concept as Supervised Market-Based Regulation.

A. *Federated Regulation (Management-Based Regulatory Delegation)*

Federated Regulation (also known as Management-Based Regulatory Delegation) is a theory for engaging private expertise in regulation both on the "front-end" (rulemaking) and on the "back-end" (compliance).[110] It

---

[109] Anecdotal evidence, such as the choice of many multi-national corporations to operate in Ireland, suggests a race-to-the-bottom among corporations operating in the E.U. to select the nation with the lowest-transaction-cost compliance procedures as their base of operations. As of the time of this writing, the authors are unaware of any comprehensive empirical study in this regard, and suggest such quantitative analysis as worthwhile future work.

[110] *See* Thaw, *The Efficacy of Cybersecurity Regulation*, *supra* note 57 at 324–26 (describing Management-Based Regulatory Delegation as having two collaborative parts; the promulgation of aspirational goals by the legislators followed by the industry experts drafting compliance plans to achieve said goals).

combines Kenneth Bamberger's theory of regulatory delegation in rulemaking[111] with Cary Coglianese and David Lazer's[112] theory of management-based regulation for compliance to describe a process which engages private expertise both to draft regulations and to allow private entities to manage their own compliance process. This process has been very successful in engaging private expertise to manage healthcare privacy and cybersecurity in the United States.[113] Under this model, legislatures establish an organic statutory framework that calls upon an administrative agency to develop regulations in conjunction with the entities subject to that regulation (and other relevant stakeholders). The regulations then promulgated by the agency, rather than defining strict standards for compliance, instead, lay out general or aspirational goals for regulated entities to achieve. Entities then are required to develop compliance plans which reasonably achieve those goals, and to follow their own plans. This last step becomes the primary compliance objective, subject to regulatory agency oversight for reasonableness of the plans and entities' adherence to those plans.[114]

Federated Regulation suggests a model both applicable to a harmonized privacy compliance process itself, and to relationships between nations and a harmonized process. The sections that follow discuss its use in these two regards.

B. *Federated Regulation Supports National Coordination Toward Harmonized Privacy Processes*

Perhaps the greatest challenge of harmonizing any aspect of E.U. and U.S. privacy regulation is the vast differences in normative conceptions of privacy among the constituent nations.[115] Federated Regulation presents one option successful at reconciling heterogeneous values into a single, functioning regulatory system.[116] Applying this approach to developing a harmonized privacy compliance regime across the U.S. and E.U. member nations presents an approach capable of developing more efficacious outcomes than the current much-criticized E.U.-U.S. Privacy Shield

---

[111] *See* Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L.J. 377, 386 (2006) (describing the delegation of regulatory authority to private firms).

[112] *See* Cary Coglianese & David Lazer, *Management-Based Regulation: Prescribing Private Management to Achieve Public Goals*, 37 LAW & SOC'Y REV. 691, 692, 725 (2003) (describing management-based regulation).

[113] *See* Thaw, *Enlightened Regulatory Capture*, *supra* note 22, 377 (presenting evidence supporting the use of private regulatory capture for public benefit).

[114] *See id.* at 362–63 (discussing how HIPAA permits covered entities to develop compliance plans conforming to its specific needs but while also penalizing for deficiencies in compliance plans).

[115] SOLOVE & SCHWARTZ, PRIVACY LAW FUNDAMENTALS, *supra* note 105.

[116] *See* Thaw, *Enlightened Regulatory Capture*, supra note 22, at 367 ("Thus rather than driving toward a least-common-denominator rule, individual parties are incentivized to cooperate with one another as much as possible.").

Agreement[117].

Under such an approach, a multi-lateral treaty would take the place of organic legislation in the Federated Regulation structure described in Section A.[118] This multi-lateral treaty would lay out aspirational goals of two forms. First, the common value of preventing privacy invasions from causing chilling effects establishes a baseline for drafting aspirational privacy goals. Second, these goals would be described in a common baseline set of positive enumerated privacy rights from the perspective of individual citizens. By focusing on positive (rather than negative) liberties, the need universally to define against which actors individuals must be protected is substantially reduced.

Rather, the "feared actors" are defined individually at the national level. Here the nations themselves take the place of the regulated entities in adopting "compliance plans" through national legislation that implements at least the core values enumerated in a multi-lateral treaty. Each nation retains its sovereign freedom to determine against which actors those rights need most strongly to be enforced to prevent the common concern of chilling effects, and each nation likewise remains free to implement additional protections.

This approach has appeal both for those who believe in the marketplace of ideas as best-equipped to resolve normative differences, as well as for those who believe that individual nations should retain sovereign power to make determinations affecting their own citizens' rights. By harmonizing compliance procedures, *procedural*-based transaction costs for organizations to operate in new jurisdictions are substantially reduced. While *substantive*-based transaction costs remain—such as an organization reassessing its information classification policy to accommodate a type of information protected as "sensitive" or "private" in a new nation, but not elsewhere—those transaction costs are exactly the types of costs the market should capture. Reducing procedural transaction costs shifts increased focus in market-participant decisions to substantive differences in privacy and data protection policies among nations, allowing the market to express global preferences regarding those policies.

Unlike command-and-control regulatory models, however, such as air pollution control regulation,[119] these policies respect the substantive choices of individual nations. By acknowledging the base levels of similarity described in Section II of this Article, the general and aspirational privacy goals articulated in a multi-lateral treaty would minimize imposition of base-

---

[117] *See* David Cole and Federico Fabbrini, *Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders*, 14 INT'L J. OF CONST. L. 220, 220–237 (2016).

[118] *See supra* Section III.A.

[119] Regulation 443/2009, 2009 O.J. (L 140) (providing emissions standards with sanctions for manufacturers that fail to meet them).

level substantive choices. While necessary to impose procedural and enforcement commonalities, such imposition under this flexible theoretical framework can provide substantial accommodation for substantive differences. While this approach does require accepting a functional and non-trivial distinction between procedural and substantive matters, in terms of the *practicalities* of privacy compliance procedures, such a distinction is not as challenging to accept as in other areas such as criminal justice.[120]

There are additional benefits to this approach as well, particularly if the procedural compliance mechanism agreed upon by the nations also uses the Federated Regulation model. Similar to the legislative debate process, the requirement that regulated entities develop compliance plans brings the issue being regulated into the risk analysis conversation at the executive management level within organizations.[121] Likewise, the Market-Supervised Regulatory Delegation model encourages similar debates in the national legislatures as they take steps to implement the general and aspirational goals required of them in the multi-lateral agreement.

Interestingly, the E.U. already appears to be using a process similar to Federated Regulation for certain pieces of legislation, for example issuing a public consultation on mobile health regulation.[122]

C. *Federated Regulation for Standardizing Compliance by Regulated Entities*

The approach to harmonizing certain core values described in section B also suggests a process for privacy compliance that nations implementing the core values of the treaty can employ. The treaty could require that nations use a Federated Regulation approach, whereby whichever entities—public or private—each nation chose to limit the privacy invasions of would be required to develop compliance plans to achieve the specific privacy

---

[120] Substance-procedure distinctions can be particularly challenging in the context of criminal justice. *See, e.g.,* Montgomery v. Alabama, 136 S.Ct. 718 (2016) (discussing the difficulties of distinguishing between procedural and substantive rules in criminal law and procedure); Miller v. Alabama, 567 U.S. 460 (2012) (same). This can be compared with the debated, but more readily accepted, distinction in U.S. administrative law, which recognizes the tension between but expressly requires distinction among procedural and substantive rules. *See* 5 U.S.C. §§ 553(b)(A) (exempting from rulemaking procedures "rules of agency organization, *procedure, or practice*) (emphasis added); *see also* Air Transp. Ass'n of America v. Dep't of Transp., 900 F.2d 396 (D.C. Cir. 1990); JEM Broadcasting Co., Inc. v. FCC, 22 F.3d 320 (D.C. Cir. 1994); Gary Lawson, FEDERAL ADMINISTRATIVE LAW 365–375 (6th ed. 2013).

[121] Smith et al., supra note 51; *see also* Thaw, *The Efficacy of Cybersecurity Regulation*, *supra* note 57, at 367 ("The risk analysis and implementation details of information security are highly technical. It is nearly impossible for senior managers, charged with overseeing the operations of an entire organization, to maintain the knowledge necessary to correct their subordinates' mistakes.").

[122] *Public Consultation on the Green Paper on Mobile Health*, DIG. SINGLE MKT., https://ec.europa.eu/digital-single-market/en/public-consultation-green-paper-mobile-health (last updated May 3, 2016, 2:45 PM).

protections laid out by that nation.

Such an approach presents a substantial advantage for transnational organizations and transnational information flow. If the privacy compliance process is the same in all nations for an organization, while it still may need to vary some of the *variables* across nations—a non-trivial business cost—a similar *process* substantially reduces compliance costs, particularly when the baseline for developing a privacy compliance plan begins with a common set of baseline criteria shared by all nations.

Lastly, it is important to note that this analysis is not a panacea, nor does it address all privacy problems. As we discuss throughout this Article, one of the potential failings of previous attempts has been the effort to solve too many (irreconcilable) problems concurrently. As noted by Professor Peter Swire, both markets and governments are limited in their ability to address privacy concerns comprehensively, particularly as a function of the barriers consumers face to expressing privacy preferences in the market or politically.[123] This proposal attempts to ease the burdens of expressing privacy protections at a macro-level, allowing nations to express preferences within a framework and letting the market sort out those preferences. It certainly is not an answer, but rather represents a possible move toward rethinking the structure of cross-border data flows in a manner which reduces *procedural* transaction costs and focuses market response more on *substantive* costs.

IV. A PROPOSAL FOR IMPLEMENTATION

One of the greatest challenges in giving effect to international agreements is the general proposition in many nations that the head-of-state (in the U.S., the President) has the unilateral authority to negotiate—and often therefore *re*-negotiate—the foreign policy of the nation at will. In the United States, presidential power in foreign affairs is nearly plenary, with the only constitutional requirement for inter-branch involvement being ratification of Treaties (but not lesser agreements) by the U.S. Senate.

As a practical matter, however, giving effect to international agreements in the United States often requires Congressional action beyond any required ratification.[124] If the agreement involves financial appropriation, for example, Congressional action may be required. If the agreement involves domestic policy within the scope of the traditional Article I powers, Congressional action likewise may be required.

Additionally, as noted above, the presidential power in U.S. foreign affairs nearly is plenary—and thus agreements are vulnerable to the shifting

---

[123] Peter W. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information* 14–15 (1997), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=11472.

[124] *See* Margot E. Kaminski, *The Capture of International Intellectual Property Law Through the U.S. Trade Regime*, 87 S. CAL. L. REV. 977, 1007 (2014) (describing how Congress has unilaterally withdrawn the U.S. from international agreements after declining to ratify them).

political winds of the current Executive. This is a particularly salient concern in an era which has seen such politically-sharp transitions as the U.S. Presidential elections of 2008 and 2016, both of which constituted electoral outcomes representing substantial shifts in foreign policy.

Privacy, by contrast, is not a concept well-suited to frequent change. Individuals make decisions based on some reasonable degree of reliance that the choices they make regarding provision of information will not subsequently be undermined as a function of downstream changes in policy. Considering the volume of information shared globally in a modern information society, it is not reasonable to expect that individuals will have the ability to control and retract each information provision they previously made. Likewise, it is not reasonable to expect that organizations—particularly for-profit private businesses—will have the capacity to build in the level of information density required to give effect to that level of version control.[125]

Thus, any international agreement, whether formally a treaty under U.S. constitutional standards, should be backed by federal legislation. Such legislation not only should create a statutory framework to ensure implementation of the agreement, but also should create "speed bumps" to ensure that any future changes do not easily reverse the reliance created among organizations and individuals on privacy choices which are difficult to reverse with adequate precision once made.

While this Article does not propose specific language for such action, we do provide a general framework sketch of one possible approach for implementing Federated Regulation to create a Market-Supervised Regulatory approach to U.S.-E.U. cross-border data flows. The core of such a framework would be a binding agreement between the U.S. and the E.U. which would include a set of basic positive assertions regarding definitions of sensitive information and data protection measures. Existing U.S. and E.U. laws do differ, in these respects, but the primary U.S. definitions of personally-identifiable information could serve as a definitional baseline of *what* is protected, and the primary E.U. requirements in the General Data Protection Regulation[126] could serve as a baseline of the *methods* of protection. These would form minimal requirements, and would become part of the implementing statutory frameworks in both U.S. and E.U. implementing legislation.

Building on this framework, which would allow for a basic degree of interoperability, a set of aspirational goals—areas to be addressed—could

---

[125] To be clear, we do not argue that businesses should not be expected to provide customized privacy settings. This, as argued by many other privacy scholars, both is a reasonable expectation and likely is in the market interests of many private actors. Such customization is, however, a scientifically-distinct concept from the highly-precise version control required to address the risks of unanticipated political change possible under contemporary approaches to foreign affairs.

[126] *See generally* Regulation 2016/679, *supra* note 40.

be defined as part of the international agreement. That agreement and the implementing statutes would then require each respective nation to consider those areas and decide—within its own political process—which additional protections (if any) to afford in the context of what data would be protected, to what degree, subject to what exceptions, and through what methods.

The agreement and implementing legislation also would specify that compliance would be achieved through a common framework. Again borrowing from the concepts of Federated Regulation, the regulatory compliance goal for each entity would be to develop a plan which addressed both the general foundational areas as well as the "additional" areas of any nation in which the entity operated. While this would create additional transaction cost as a function of *substantive* protections, the transaction cost of operating in an additional nation would be minimal as a function of *compliance* cost, since the same methods of demonstrating compliance would apply.

The goal here is not to achieve substantive convergence nor is it to reduce substantive compliance costs. Rather, it is to allow the function of the market and the political process to sort out which private protections apply. A regime of this nature would preclude a "race-to-the-bottom" as some argue currently occurs in the E.U., and likewise would close the "black hole" of the Safe Harbor/Privacy Shield. If a nation's privacy protections become "too costly" and organizations elect not to conduct business there, that nation's political process would be faced with the choice of revising their protections or losing access to international services. Likewise, nations no longer could serve as safe havens for lower privacy protections below what would ordinarily be demanded by the market or by political processes.

CONCLUSION

Privacy in cross-border data flows is one example of a larger problem. Much like the challenge of the radio spectrum, privacy of postal mail, wiretapping, and early Internet questions, over time societal and market developments will change the nature and scope of the problem. What will remain constant is the need for theoretical frames through which policymakers can develop regulatory frameworks for dealing with rapidly changing technology. The historical examples listed above, and many others discussed in related jurisprudence and scholarship both in the U.S. and the E.U., demonstrate well the accelerating trend of technological change outpacing legal and policy processes.

This outpacing is not inherently evil, as the law does (and arguably should) respond carefully, contemplatively, and with care—all things to which speed is anathema. Yet rapidly-developing technology remains. What then must a society do? This Article presents the concept of Market-Supervised Regulatory Delegation as a method of allowing policymaking to embrace the market—which will continue to develop regardless of the speed

at which the law responds—and rather than distorting market outcomes, seek to enhance the degree to which the market expresses preferences across nations with differing normative priors but where the question at issue is inherently internetworked, and therefore international.

Stated far more simply—this proposal allows the market to function, preserves national sovereignty, without sacrificing the benefits of international trade. We hope others will critically examine, critique, build upon, and improve it as a potential approach for international regulation of complex, rapidly-changing technological markets.

Finally, we note that in the specific context of privacy and cross-border data flows, this Article is exploratory and seeks to lay out a theoretical framework. That framework considers whether it is possible to harmonize the *process* of privacy compliance in different regimes without having to reach agreement on all aspects of the substance of that regulation. Such a distinction does not ignore the well-established debate over whether procedural and substantive rules can be differentiated, but rather elects the assumption that they can and explores whether doing so may yield fruit to improve a currently undesirable and inefficient regulatory outcome. We recognize that this proposal is far from a policy directive, but hope that its framework encourages policymakers on both sides of the Atlantic to consider new perspectives both on what should be the goals of cross-border data flow policy and what styles of regulatory frameworks can be employed to achieve those goals.