Bloomberg BNA

Privacy and Security Law Report®



# Defining 'Personal Data' in the European Union and U.S.

BY PAUL M. SCHWARTZ AND DANIEL J. SOLOVE

The applicability and scope of many privacy laws around the world depend upon how the term ''personal data'' is defined. Personal data is often referred to as ''personally identifiable information'' (PII), and we use the terms interchangeably here.[1] PII is foundational to any privacy regulatory regime in its role of a jurisdictional trigger. In the U.S., privacy laws apply when PII is involved and are inapplicable when PII isn't involved. The concept of personal data plays a similar role in the privacy law of the European Union. In the absence of personal data, there is no privacy right.

Given PII's fundamental role in privacy law, it is surprising that it lacks a uniform definition. In previous work, we focused on the approach to PII in U.S. privacy law and criticized the law's disjointed, inconsistent and often overly narrow definitions of PII. To make privacy law effective for the future, we developed a new conception, PII 2.0, which avoids the problems and pitfalls of current approaches. The key to our model is to build three categories of PII—(1) identified, (2) identifiable or (3) non-identifiable—and to treat them differently.[2] This approach permits tailored legal protections built around different levels of risk to individuals.

In this article, we argue that PII 2.0 can do more than serve as the most workable approach for U.S. privacy law. It would also function well for EU privacy law and help harmonize the significantly divergent approaches between U.S. and EU privacy law.

[1] The term ''PII'' is more frequently used in the U.S. The term ''personal data'' is more frequently used in the European Union.

*This is an abridged version of a law review article published by the California Law Review. See Paul M. Schwartz & Daniel J. Solove, Reconciling Personal Information in the United States and European Union, 102 Calif. L. Rev. 877 (2014), available at http://ssrn.com/abstract=2271442.*

*Paul M. Schwartz is Jefferson E. Peyser professor of law at the University of California, Berkeley School of Law and director of the Berkeley Center for Law & Technology. He is also a special adviser at Paul Hastings LLP in San Francisco.*

*Daniel J. Solove is the John Marshall Harlan research professor of law at George Washington University Law School. He is also senior policy adviser at Hogan Lovells US LLP, in Washington, and founder of TeachPrivacy, http://teachprivacy.com, a company that provides computer-based privacy and data security training for a wide variety of companies and organizations.*

## I. Defining PII in the EU and U.S.

In the EU, the current framework for defining personal information includes both the Data Protection Directive (95/46/EC) (''Directive''), which was enacted in 1995,[3] and the proposed General Data Protection Regulation (''Proposed Regulation''), which was released in 2012[4]—the final form of which EU institutions are currently debating. Under both the Directive and Proposed Regulation, the EU takes a broad approach to defining PII. The definition turns on whether a natural person is capable, whether directly or indirectly, of identification

[2] Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. Rev. 1814, 1877–82 (2011) (11 PVLR 142, 1/23/12).

[3] Directive 95/46/EC, of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 7, 1995 O.J. (C 93) [hereinafter Data Protection Directive].

[4] Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation) (Jan. 25, 2012) [hereinafter Proposed Regulation] (11 PVLR 178, 1/30/12).

 ISSN 1538-3423

through a linkage or some other reference to available data. In the EU, information that is identified or identifiable receives an equivalent level of legal protection. In the U.S., in contrast, there is not a single definition of PII, but three different definitional approaches.

### A. The EU Data Protection Directive

The EU Data Protection Directive uses the term ''personal data'' and defines it as ''information relating to an identified or identifiable natural person.''[5] The Directive does not explicitly define ''identified.'' Under an EU directive, the law of member states then becomes determinative. In the definition of EU member states that traditionally have taken a leading role in information privacy law, a person falls in the ''identified'' category if a party can use information relating to her to determine her specific identity.

The EU Data Protection Directive is more specific regarding its definition of ''identifiable.'' It explains that 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.''[6] As additional definitional assistance, the Directive in its Recital 26 explains that in determining whether a person is identifiable, ''account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.''[7]

Both identified and identifiable information fall squarely within the scope of EU data privacy law, and they are treated in the same fashion. From the U.S. perspective, the resulting EU legal regime is formidable both in terms of the protection granted to the affected individual, the data subject and the duties placed on the party who processes the personal information.

### B. The Proposed Regulation

The EU is now in the process of replacing the Directive with the Proposed Regulation. In January 2012, the European Commission released a draft version of this document, its proposed General Data Protection Regulation.[8] This development marks an important policy shift. While a directive requires member states to pass harmonizing legislation that ''transposes'' its standards into national law, a regulation establishes directly enforceable standards.

The Proposed Regulation generally builds on the approach of the Directive, but contains some notable changes. Instead of a concept of ''identified'' or ''identifiable,'' it first defines personal data as ''any information relating to a data subject.''[9] The nature of the ''relating to'' requirement is further specified in the definition of ''data subject.'' The Proposed Regulation states that a data subject is a person who ''can be identified, directly or indirectly, by means reasonably likely to be used.''[10] Thus, the Proposed Regulation shifts from the Directive's notion of identified or identifiable to a concept of direct or indirect identification.

At the same time, however, there is important continuity in the concept of ''means reasonably likely to be used.'' The ultimate test regarding ''identifiability'' (Directive) or indirect identification (Proposed Regulation) is the same. An analysis must consider ''all the means likely reasonably to be used either by the controller or by any other person to identify'' the individual.[11] The repetition of the language in both documents indicates that when determining whether personal data exist in the EU, one must consider the likelihood that certain steps, such as combining bits of scattered data or reidentifying non-personal information, will be taken.

The breadth of the EU approach has both benefits and drawbacks. The primary benefit is that hardly anything escapes EU privacy regulation. There are few gaps and inconsistencies under the EU approach, a stark contrast to the U.S. approach where such gaps and inconsistencies are legion. But there is also a primary drawback to the EU approach. Under both the Directive and Proposed Regulation, information is treated as the same whether it refers to an identified individual, or one who can be ''indirectly identified''—that is, someone who the Directive terms ''identifiable.'' All these terms constitute personal data, and their presence activates the ''on'' switch for triggering a full suite of obligations and protections. Yet, a broad continuum of identifiable information exists, and it includes different types of anonymous or pseudonymous information. Moreover, different levels of effort are required to identify information, and various risks are associated with the possible identification of data. Placing all such data into the same conceptual category as ''data that currently relate to an identified person'' risks activating burdensome regulations for data processing entities.

### C. The U.S.: A Lack of a Uniform Standard

Instead of defining personal information in a coherent and consistent manner, privacy law in the U.S. offers multiple competing definitions. In U.S. law, there are three predominant approaches to defining personal information. These are (1) the ''tautological'' approach, (2) the ''non-public'' approach and (3) the ''specific-types'' approach.[12]

The tautological approach is an example of a standard, or an open-ended decision-making tool. Under the tautological approach, U.S. privacy law simply defines ''personal'' as meaning any information that identifies a person. The Video Privacy Protection Act of 1988 (VPPA) neatly demonstrates this model.[13] The VPPA, which safeguards the privacy of video sales and rentals, defines ''personally identifiable information'' as ''information which identifies a person.''[14] For purposes of the statute, information that identifies a person becomes ''personal identifiable information'' and falls

[5] Data Protection Directive, *supra* note 3, at art. 2(a).
[6] *Id.*
[7] *Id.* at recital 26.
[8] For an introduction to the Proposed Regulation, *see* Paul M. Schwartz, *The EU-US Privacy Collision: A Turn to Institutions and Procedures*, 126 Harv. L. Rev. 1966, 1992–200 (2013).
[9] Proposed Regulation, *supra* note 4, at art. 4(2).
[10] *Id.* at art. 4(1).
[11] *Id.* at recital 23; Data Protection Directive, *supra* note 3, at recital 26.
[12] Schwartz & Solove, *supra* note 2, at 1828–36.
[13] 18 U.S.C. § 2710 (2006).
[14] *Id.* § 2710(a)–(b). The VPPA prohibits ''videotape service providers'' from knowingly disclosing personal information, such as the titles of items rented or purchased, without the individual's written consent. It defines ''videotape service providers'' in a technological neutral fashion to permit the law to be extended to DVDs. *Id.* § 2710(a)(4).

  PVLR ISSN 1538-3423

under the statute's jurisdiction if tied to the purchase, request or obtaining of video material.

A second model focuses on non-public information. The non-public approach seeks to define personal information by focusing on what it is *not* rather than what it is. The non-public approach excludes from its protected scope any information that is publicly accessible or that is purely statistical. The relevant legislation does not explore or develop the logic behind this approach, but rather simply concludes that information falling in these categories is not personal information. The Gramm-Leach-Bliley Act of 1999 epitomizes this approach by defining ''personally identifiable financial information'' as ''nonpublic personal information.''[15]

The third approach of U.S. privacy law is to list specific types of data that constitute personal information. In the context of the specific-types approach, if information falls into an enumerated category, it becomes per se personal information under the statute. State data breach notification laws take this approach. These statutes, which 47 states have now enacted, require a business to notify affected individuals should an information security breach occur.[16]

These laws generally define personal information through the specific-types approach.[17] As an illustration, the Massachusetts breach notification statute requires that individuals be notified if a specific set of their personal information is lost or leaked.[18] To complicate the lives of lawyers handling multistate data breaches, other state statutes contain different lists of enumerated types of information that constitute PII.[19]

One can also point to a broader flaw in the approach of U.S. law to PII. As a general rule, PII in the U.S. is largely limited to instances where data refer to an *identified* individual. The typical U.S. approach is represented by the many state breach notification laws. In these statutes, personal information is limited to identified data: namely, a first name or initial and a last name, plus information from a specific list of the kinds of data that will make identification certain.

## II. Personal Information: A Problem on Both Sides of the Atlantic

The approaches to defining PII in the U.S. and in the EU are all flawed in significant ways. Stated succinctly, we find the EU approach to be too expansionist and the U.S. approach too reductionist, with problematic consequences flowing from both techniques. Moreover, the divergence between these approaches raises the threat of destabilizing the current privacy status quo between the U.S. and EU. The stakes in this area of law are high because the trans-Atlantic free flow of data depends on coordination between the two legal systems.

If PII or personal data were a small dimension of privacy regulation, such problems might be isolated and worked around. But the definition of PII is a foundational issue that implicates the scope of privacy regulation. Before even considering differences in *how* data are protected in the U.S. and EU, we must address differences in *what* data are protected under these two privacy regimes. This state of disarray points to the critical importance of revising the definition of PII in the U.S. and EU alike.

The disjunction between U.S. and EU definitions of PII also raises problems regarding the harmonization of the privacy law of these two systems. Just as the differing legal definitions of PII within the U.S. raise compliance costs for U.S. companies, the differing approaches between the EU and U.S. further heighten regulatory uncertainty. Information that is ''identifiable'' in the EU and, hence, subject to Article 25 of the Directive, or ''indirectly identified'' and hence subject to the Proposed Regulation, may not be subject to privacy law in the U.S. As a consequence, international companies face complex legal decisions when designing software, services or devices for use in both the EU and U.S.

Furthermore, the different definitions of PII threaten the current status quo around second-order mechanisms for allowing data transfers. These are the U.S.-EU Safe Harbor Program, Model Contractual Clauses and Binding Corporate Rules. If the EU and U.S. cannot agree on a definition of PII, the most basic unit of information privacy law, these processes must be seen as essentially instable.

## III. PII 2.0

The existing definitions of personal information, whether in the EU or U.S., are problematic. We propose a new conception of PII called PII 2.0, and below, we explain how this new conception can bridge significant differences in EU and U.S. privacy law.

### A. An Explanation of PII 2.0

PII 2.0 places information on a continuum. On one end of the continuum, there exists no risk of identification. At the other end, an individual is fully identified. We divide this continuum into three categories, each with its own regulatory regime. Under the PII 2.0 model, information can be (1) identified, (2) identifiable or (3) non-identifiable. Because these categories do not have hard boundaries, we define them in terms of standards, as open-ended benchmarks rather than hard-edged rules.

#### 1. Identified Data

Information refers to an *identified* person when it singles out a specific individual from others. Put differently, ascertaining a person's identity makes her identified. There is general international agreement about the content of this category, albeit not of the implications of being placed in it.

There are also certain instances where *identifiable* information should be treated like information referring to an *identified* person. Information that brings a substantial risk of identification of an individual should be treated as referring to an identified person. In other words, identifiable data should be shifted to the *identified* category when there is a significant probability that a party will make the linkage or linkages necessary to identify a person. This essential subcategory requires assessment of the means likely to be used by parties with current or probable access to the information, as well as the additional data upon which they can draw.

[15] 15 U.S.C. § 6809(4)(A) (2006).
[16] *See* Daniel J. Solove & Paul M. Schwartz, *Privacy Law Fundamentals* 176–78 (2013).
[17] *See id.* at 17–74.
[18] Mass. Gen. Laws Ann. ch. 93H (West 2007).
[19] Solove & Schwartz, *supra* note 16, at 176–78.

This test, like those for the other categories, is a contextual one.

In essence, this category of PII is at the high end of the spectrum in terms of the likelihood it will be identified to a person.

#### 2. Identifiable Data

Information in the middle of the PII 2.0 risk continuum relates to an *identifiable* individual when specific identification, while possible, is not a significantly probable event. The likelihood for identification is low to moderate.

An example of *identifiable* information under the PII 2.0 model would be the key-coded medical data that the EU Article 29 Working Party discussed in its ''Opinion on the Concept of Personal Data.''[20] Some or all of this information might never be identified. Depending on the risk scenario, there may be only a remote chance of future linkage to a specific person.

For an example from the U.S. regarding ''identifiable'' but not ''identified'' information, we turn to the Federal Trade Commission staff report, ''Protecting Consumer Privacy in an Era of Rapid Change.''[21] This report considers the issue of when information is ''reasonably linkable'' to a person.[22] Citing to our previous work on PII 2.0, the FTC noted that businesses can sometimes re-identify non-PII data and often have incentives to do so.[23] The FTC argued that if companies take three specific steps to minimize linkability, the information should be viewed as non-PII.[24] First, the company must use reasonable means to ensure that the data is de-identified, or cannot be tied to a specific consumer.[25] Second, the company must publicly commit that it will use the data only in de-identified fashion and not attempt to re-identify it.[26] Finally, if the company makes the de-identified data available to other companies, it must contractually bind the other entities to avoid re-identifying the data and to engage in reasonable oversight to monitor compliance with these contracts.[27] These steps demonstrate a practical policy for maintaining information in the identifiable category.

#### 3. Non-Identifiable Data

At the other end of the continuum, *non-identifiable* information carries only a remote risk of identification. Such data are not relatable to a person, taking account of the means reasonably likely to be used for identification. In certain kinds of data sets, for example, the original sample is so large that other information will not enable the identification of individuals. A simple example of non-identifiable information is high-level information about the populations of the U.S., China and Japan, and their relative access to telecommunications.

Practical methodologies now exist for assessing the risk of identification. In fact, computer scientists have developed metrics for assessing the risk of identifiability of information. For example, Khaled El Emam has identified benchmarks for assessing the likelihood that de-identified information can be linked to a specific person—that is, can be made identifiable.[28]

### B. PII 2.0 and Fair Information Practices

Our reconceptualized notion of personal information places greatest emphasis on the likelihood of potential identification. PII 2.0 conceives of identifiability as a continuum of risk rather than as a simple dichotomy. We have three categories rather than a binary so that privacy law can function in a more nuanced and practical way to the likelihood of identifiability.

In the U.S. and EU, there is a binary approach to privacy regulation. If there is PII, then the regulation applies in full force. If there isn't PII, then the regulation doesn't apply. Our model envisions a more modulated approach.

In the *identified* category, a full slate of privacy protections should apply. These protections are commonly known as the Fair Information Practice Principles (FIPPs), and they include: (1) limits on information use; (2) limits on data collection (also termed ''data minimization''); (3) limits on the disclosure of personal information; (4) collection and use only of information that is accurate, relevant and up-to-date (''data quality principle''); (5) notice, access and correction rights for the individual; (6) creation of processing systems that the concerned individual can know about and understand (transparent processing systems); and (7) security for personal data.[29]

In the *non-identifiable* category, the FIPPs should not apply. Instances involving non-identifiable data are not ones involving privacy. Non-identifiable data should be treated as akin to general data. There may be other laws to regulate certain types of data, but privacy is implicated when data *about individuals* is involved.

As for the category of *identifiable* information, it is here where our proposal differs significantly from current law in the U.S. and EU. In the U.S., the law often treats identifiable information as falling outside of the scope of privacy law. In the EU, the law treats identifiable information as the complete equivalent to identified information. We contend that the law should treat identifiable information in a different way. Identifiable information should not be treated the same as non-identifiable information because there are risks of linkage to specific people. Identifiable information should also not be treated as fully equivalent to identified information. The information does not yet refer to a specific person and may never do so. We therefore propose that identifiable information should be protected by some of the FIPPs, but not all of them.

In thinking about FIPPs for identifiable data, the easiest starting point is to eliminate inapplicable categories.

---

[20] Article 29 Working Party, *Opinion 4/2007 on the Concept of Personal Data*, WP136, 19 (June 20, 2007).

[21] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers* (Mar. 2012) (11 PVLR 590, 4/2/12)(11 PVLR 590, 4/2/12).

[22] *See id.* at iv.

[23] *Id.* at 20.

[24] *Id.* at 20–21.

[25] *Id.* at 21.

[26] *Id.*

[27] *Id.*

[28] *See* Khaled El Emam, *Guide to the De-Identification of Personal Health Information* 151–58 (2013); Khaled El Emam, *Heuristics for De-Identifying Data*, Security & Privacy, July/Aug. 2008, at 58; Khaled El Emam, *Risk-Based De-Identification of Health Data*, Security & Privacy, May/June 2010, at 64.

[29] *See, e.g.*, Org. for Econ. Co-operation & Dev. [OECD], *Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD Doc. C(80)(58) final (Oct. 1, 1980), reprinted in 20 I.L.M. 422, *available at* http://bit.ly/1lWG9Qk.

  PVLR ISSN 1538-3423

Full notice, access and correction rights should *not* be granted to an affected individual simply because identifiable data about her are processed. For one thing, if the law created such interests, these obligations would perhaps decrease rather than increase privacy by requiring that all such data be associated with a specific person. This result follows because entities would need to maintain an ongoing connection between the individual and the identifiable information to allow that individual to exercise her rights of notice, access and correction. In this fashion, the law's implementation could force the transformation of *identifiable* data into *identified* data. Article 10 of the Proposed Data Protection Regulation explicitly seeks to avoid this result. It provides that a data controller is not obligated to collect further information in order to identify the data subject for the mere purpose of complying with the Proposed Regulation.[30]

Moreover, limits on information use, data minimization and restrictions on information disclosure should not be applied across the board to identifiable information. Such limits would be disproportionate to risks from data use and would cripple socially productive uses of analytics that do not raise significant risks of individual privacy harms.[31] Among non-consumer use of analytics, analysis of large data sets plays an increasingly important role in health-care research, the management of physician performance and clinical metrics, data security and fraud prevention.

As noted above, while all FIPPs should not apply to identifiable data, there are three that are applicable in this context. The key FIPPs are those that concern data security, transparency and data quality. Data security refers to the obligation to ''protect against unauthorized access to and use, destruction, modification, or disclosure of personal information.''[32] Identifiable information should be subject to data security principles. Recall that identifiable data are those for which a specific identification, while possible, is not a significantly probable event. Yet these data, unlike non-identifiable information, might be relatable to a person. Data security for identifiable information, as for identified information, should be commensurate with the nature of the information and the likely risks of disclosure.

The transparency FIPP calls for the creation of data processing systems that are open and understandable to affected individuals. Openness about information use allows for improved policies and law. Moreover, transparency about the collection of identifiable information will heighten awareness about data flows among all parties, both consumers and corporations. It will thereby improve the position of consumers who have preferences about the collection and further use of data—even should that information merely be identifiable.

Finally, data quality is a FIPP that requires organizations to engage in good practices of information handling. This requirement depends on the purpose for which information is to be processed. In the context of *identified* data, for example, the greater the potential harm to individuals, the more precise the data and data processing must be. In the context of *identifiable* information, data quality also requires good practices of information handling. In particular, it requires that companies pay attention to the use and processing of identifiable information by third parties. If information is non-identifiable, a company can publicly release it or permit third parties access to it without further obligations.

Identifiable information is capable of identification, even if this risk is not significantly probable. Thus, companies cannot merely release or allow unmonitored access to it. Depending on the potential harm to individuals and the likely threat model, companies should also be required to use a ''track and audit'' model for some identifiable information.[33] An example is information used in health-care research. Access to such data should be accompanied by legal obligations that travel with the information.

## IV. PII 2.0 and EU Privacy Law

Our PII 2.0 approach would regulate personal data with more nuance and would avoid the current inconsistencies and incoherence in the law. PII 2.0 would also serve as a bridge between U.S. and EU privacy law. PII 2.0 attempts to align U.S. and EU privacy law by using concepts derived from each. From the U.S. approach, PII 2.0 takes a more harm-based approach. Like U.S. law, it gives data about identified individuals the most protection. Like EU law, PII 2.0 recognizes that identifiable data still deserve protection and should be included within the definition of PII.

In our view, PII 2.0 is not only fully compatible with the EU approach, but it is also consistent with the underlying philosophy of the EU towards privacy. The EU might view protecting identifiable data with fewer FIPPs as a retreat from its current approach where such data are protected by all the FIPPs. However, PII 2.0 actually enhances the protection of privacy—even in the EU. PII 2.0 creates an incentive for companies to keep information in its least identifiable form. By treating identified and identifiable information as equivalents, companies will be less willing to expend resources to keep data in the most de-identifiable state practicable. They would also be less likely to develop strong contracts with outside parties to keep shared information de-identified, as the FTC proposes.[34] Thus, PII 2.0 will ultimately improve privacy protections by creating a robust incentive for companies to maintain data in identifiable form rather than identified form.

There is a foundation in EU privacy law for such an approach to be embraced. The Proposed Data Protection Regulation and the Article 29 Working Party indicate that the full requirements of EU data protection law need not apply to all types of personal data, whether identified or identifiable information. At present, however, while this evidence does not represent the conventional wisdom, it provides some support for the evolution of the majority view. As mentioned previ-

[30] Proposed Regulation, *supra* note 4, at art. 10.

[31] At the Article 29 Working Party of the EU, there recently has been openness to a concept of proportionality in the use of information privacy law. *See* Article 29 Working Party, *Opinion 3/2010 on the Principle of Accountability*, WP 173, 3 (July 13, 2010) (9 PVLR 1063, 7/19/10). The question remains as to how successful this concept can be in a system that treats identified and identifiable data as equivalents.

[32] Lisa J. Sotto, *Privacy and Data Security Law Deskbook* § 14.02 (2011).

[33] Paul Ohm, *Broken Promises of Privacy*, 57 U.C.L.A. L. Rev. 1701, 1741–42 (2010).

[34] *See* FTC, *supra* note 21, at 21.

ously, the Proposed Regulation recognizes that applying its full requirements to identifiable data would create, at least at times, the perverse result of obligating organizations to collect more personal data in order to authenticate the data subjects. The drafters therefore wisely included Article 10, which provides that data controllers need not collect more personal information to identify the data subject for the mere purpose of complying with the Proposed Regulation.[35]

## V. Conclusion

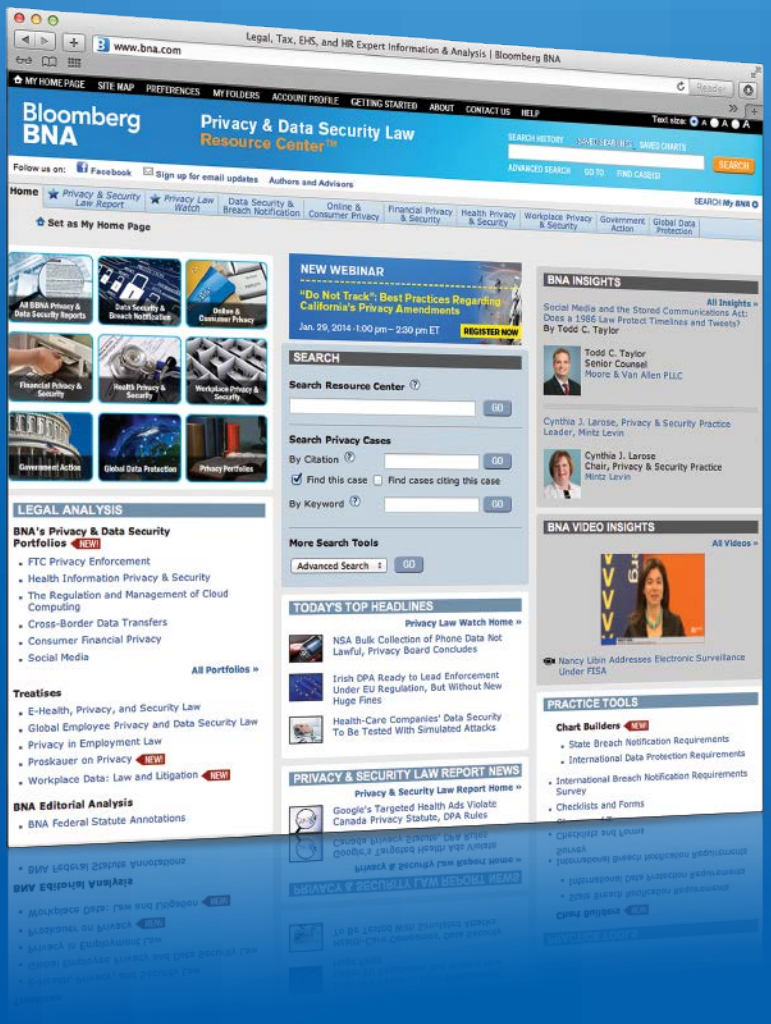
Despite the divergence between the concepts of personal data in the U.S. and the EU, the differences between the two systems can be reconciled to a certain extent. PII 2.0 rationalizes the currently inconsistent U.S. approach to defining personal data. It also is compatible with basic principles of U.S. privacy law by focusing on the risk of harm to individuals. PII 2.0 is consistent as well with the acknowledgment of EU privacy law of the need to provide different categories of information with different kinds of protection. In the EU, it would provide for more tailored and nuanced protection. Most importantly, in both the EU and U.S., it would enhance the protection of privacy by creating an incentive for companies to keep information in the least identifiable form. PII 2.0 would be an ideal starting point toward reconciling these divergent bodies of law.

[35] Proposed Regulation, *supra* note 4, at art. 10.

  PVLR ISSN 1538-3423

**NEW PORTFOLIOS & TREATISES NOW AVAILABLE**

# SAFE DATA & SOUND SOLUTIONS




## Privacy & Data Security Law Resource Center™

Unparalleled news. Expert analysis from the new Privacy & Data Security Portfolio Practice Series. Comprehensive new treatises. Proprietary practice tools. State, federal, and international primary sources. The all-in-one research solution that today's professionals trust to navigate and stay in compliance with the maze of evolving privacy and data security laws.

**TO START YOUR FREE TRIAL CALL 800.372.1033 OR GO TO www.bna.com/privacy-insights**

Bloomberg BNA