2015

Privacy and Health Information: The United States and the European Union

Leslie Francis
University of Utah

Follow this and additional works at: <https://uknowledge.uky.edu/klj>

Part of the [Health Law and Policy Commons](#), and the [Privacy Law Commons](#)

[Right click to open a feedback form in a new tab to let us know how this document benefits you.](#)

Recommended Citation

Francis, Leslie (2015) "Privacy and Health Information: The United States and the European Union,"
Kentucky Law Journal: Vol. 103: Iss. 3, Article 7.

Available at: <https://uknowledge.uky.edu/klj/vol103/iss3/7>

This Article is brought to you for free and open access by the Law Journals at UKnowledge. It has been accepted for inclusion in Kentucky Law Journal by an authorized editor of UKnowledge. For more information, please contact UKnowledge@lsv.uky.edu.

Privacy and Health Information: The United States and the European Union

*Leslie Francis*¹

INTRODUCTION

Pandemics urgently remind us of the need for health information. Without sufficiently accurate and comprehensive information, identification of disease outbreaks may be delayed to the point that containment becomes far more difficult. But the need for health information is not limited to contagious disease, the original focus of public health surveillance. Health information is also critical for the analysis and comparison of population health trends, for comparisons of cost and quality of care, and for comparative assessments of treatment efficacy. Information in patient records and other health information may also be crucial for research on both existing and novel treatment modalities. Moreover, it may help us understand the natural course of diseases or complex relationships between genotypes and phenotypes. With large data sets of health information, it is also possible to identify rare side effects of medication or drug interactions.

Although public health information is typically collected by entities that track political jurisdictions, the need for such information transcends borders. In order to identify and track disease outbreaks or other potential events of concern to public health, data on an international scale may be crucial. Cross-border comparisons of treatment costs, efficacy, or quality may prove illuminating. Especially for the detection of less frequent events in subpopulations, data from more than one jurisdiction may be required. If jurisdictions have significantly different legal structures for data protection, however, the benefits of shared data may not be attained.

The United States (US) and the European Union (EU) both have extensive systems for the collection of health information that can be important for many purposes. However, they have significantly different legal structures for data protection. These differences are likely to persist or intensify if the EU finalizes proposed changes to its data protection regime. This article describes the differences between EU and US legal protections for health information. It urges institutionalization of protections that allow both the EU and the US to share health information in a manner consistent with their commitments to individual privacy.

¹ Distinguished Alfred C. Emery Professor of Law and Distinguished Professor of Philosophy, University of Utah.

As described below, EU data protection rests primarily in the Charter of Fundamental Rights and Freedom and with Directive 95/46/EC. The latter is currently in the final stages of a revision process. Each member state has its own data protection legal structure that must meet these over-arching requirements. Data protection in the U.S. is far more fragmented, including the federal Privacy Act for data possessed by the federal government, state data protection laws, the Health Insurance Portability and Accountability Act (HIPAA) protections for health information possessed by entities it covers, the Federal Trade Commission prohibition of unfair or deceptive trade practices, and many other federal and state laws involving different types of data or data holders. The focus in the discussion to follow will be EU and US federal data protection laws, rather than the laws of the various sub-jurisdictional units.

I. IDENTIFIABLE AND NON-IDENTIFIABLE HEALTH INFORMATION

On both sides of the Atlantic, data protection laws apply to information that might identify individuals. For example, the EU Directive 95/46 defines “personal data” as “any information relating to an identified or identifiable natural person.”² In the United States, the HIPAA statute and accompanying rules apply to “health information,” that is, information that relates “to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.”³ There are many reasons for the structure of HIPAA, including the concerns about individual harm and respect for individual choice that underlie the impetus for data protection.⁴ An advantage of this structure is that de-identified or never-identified information can be shared outside of the requirements of jurisdictions’ data protection laws.⁵

However, the distinction between identifiable and de-identified data is increasingly difficult to implement in practice.⁶ Some information—such as genetic information, radiology scans, or cardiac tracings—may be unique to a particular individual.⁷ Even if proper de-identification procedures are followed, combinations of data may permit identification of unique individuals to a high degree of probability.⁸ The advent of the “Internet of Things”—especially smart devices worn

² Council Directive 95/46, art. 2(a), 1995 O.J. (L 281) 38 (EC).

³ 45 C.F.R. § 160.103 (2014).

⁴ See U.S. Dep’t of Health & Human Servs., Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators, 76 Fed. Reg. 44,512, 44,513–14, 44,524 (July 26, 2011).

⁵ See *id.* at 44,525.

⁶ See *id.* at 44,524.

⁷ Recognizing this, the proposal for changing the U.S. Common Rule for the protection of human research subjects suggested treating all genetic information as identifiable. See *id.* at 44,526.

⁸ See Melissa Gymrek et al., *Identifying Personal Genomes by Surname Inference*, 339 SCI. 321, 324 (2013).

on the person—may render anonymous collection of data increasingly a thing of the past.⁹

Moreover, some of the benefits of data sharing can be realized with anonymous or de-identified data, but many cannot. Identifiers are needed at some stage in the process if records are to be linked reliably. If there is any reason to re-contact individuals, for example, for contagious disease contact tracing or information about identified health risks, identifiers will also be necessary. If information is to be analyzed in such a way that it covers small areas or involves cells in which there are very small numbers—as might be the case for rare conditions—inferences about individuals may also be possible.

Significant controversy remains about the acceptable levels of risks of re-identification and how these risks can be mitigated.¹⁰ Controversy also exists about whether de-identification is sufficient protection even if it could be implemented reliably.¹¹ Labels applied to groups may stigmatize those groups, and uses of de-identified data may be thought to violate the integrity of individuals from whom the data were originally collected, even if they no longer can be identified.¹² These issues surrounding de-identification will remain even if practices for the treatment of identifiable information are improved, but they are set aside for the remainder of this discussion.

II. DATA PROTECTION LAW IN THE EU

The EU has both Union-wide and individual member state data protection laws. At the level of the EU, overarching protections apply to all data types within the scope of EU's power to regulate, power that remains limited under basic EU law.¹³ The Lisbon Treaty requires the Union to respect the equality and national identities of member states.¹⁴ It reserves specified functions to member states, especially the function of national security but also the functions of ensuring the territorial integrity of the state and maintaining law and order.¹⁵ The Treaty also endorses the principle of subsidiarity, meaning that in areas not within its exclusive competence, the Union acts only to the extent that the objectives of the proposed

⁹ Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things, at 4, 14/EN, WP 223 (Sept. 16, 2014), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

¹⁰ See generally Russ B. Altman et al., *Data Re-Identification: Societal Safeguards*, 339 SCI. 1032, 1032–33 (2013) (acknowledging that re-identification is a problem for unique individuals and advocating for increased regulatory measures); Gymrek et al., *supra* note 8, at 321–24 (reporting a study of re-identification for American men).

¹¹ See generally Altman, *supra* note 10; Gymrek, *supra* note 8.

¹² See, e.g., Mark A. Rothstein, *Is Deidentification Sufficient to Protect Health Privacy in Research?*, AM. J. BIOETHICS, Sept. 1, 2010, at 3, 6–7.

¹³ See Consolidated Version of the Treaty on European Union art. 4, Sept. 5, 2008, 2008 O.J. (C115) 18 [hereinafter Treaty of Lisbon].

¹⁴ *Id.*

¹⁵ See *id.* arts. 4–5.

action cannot be sufficiently achieved by member states acting separately but instead can be better achieved at Union level.¹⁶

The fundamentals of EU data protection law are set out in the Charter of Fundamental Rights.¹⁷ Effective in 2009, the Charter institutionalizes protection of certain basic rights as a matter of fundamental EU law.¹⁸ Among these rights are the Article 1 right to human dignity, the Article 3 right to the integrity of the person including free and informed consent to medical interventions, the Article 6 right to liberty and security of the person, the Article 7 right to respect for private and family life, and the Article 8 right to protection of personal data.¹⁹ This last right includes the general right to protection of personal data and the more specific rights that personal data will 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.”²⁰ Article 8 also provides that everyone has the right to access data about himself or herself and the right to rectification of data.²¹ Compliance with Article 8 must be subject to oversight by an independent authority.²²

Directives under EU law set out basic requirements that member states must implement in their national laws. Individual member states have considerable latitude to determine how they will achieve compliance with a directive. Directive 95/46, adopted now almost twenty years ago, set out a framework for data protection in order to further the free movement of information among EU member states.²³ The concern giving rise to the Directive was that member states were increasingly unwilling to allow data transfers out of concerns that privacy would not be adequately protected.²⁴ Following the principle of subsidiarity, the Directive requires all member states to determine the circumstances under which the processing of personal data is lawful in accord with Directive requirements.²⁵

The Directive applies to all processing of personal data by automatic means or by means of a filing system.²⁶ Requirements of the Directive are applied to “data controllers,” who determine the purposes and means of collecting and processing personal data, and to “data processors,” entities processing data on behalf of controllers.²⁷ Data controllers and processors may be natural persons, legal persons such as corporations, or public entities.²⁸

¹⁶ *Id.* art. 5.

¹⁷ Charter of Fundamental Rights of the European Union art. 8, Dec. 18, 2000, 2000 O.J. (C364) 10 [hereinafter Charter of Fundamental Rights].

¹⁸ *See generally id.* pmb.

¹⁹ *Id.* arts. 1, 3, 6–8.

²⁰ *Id.* art. 8, para. 1–2.

²¹ *Id.* para. 2.

²² *Id.* para. 3.

²³ *See generally* Council Directive 95/46, pmb. ¶ 3, 1995 O.J. (L 281) 31 (EC).

²⁴ *See id.* pmb. ¶ 5.

²⁵ *Id.* art. 5, at 39.

²⁶ *Id.* art. 3(1).

²⁷ *See id.* art. 2(d), (e), at 38.

²⁸ *Id.*

The Directive does not apply to the processing of personal data outside the scope of EU law, including the processing of personal data for purposes of national security, defense, or criminal law enforcement.²⁹ It also does not apply to processing by a natural person for household activities.³⁰ Member states must provide exemptions for data processing carried out solely for journalism, artistic, or literary expression, but “only if [these exemptions] are necessary to reconcile the right to privacy with rules governing freedom of expression.”³¹

The Directive requires EU member states to require that personal data must be processed fairly and lawfully. Data must be collected for specified purposes.³² Data must be kept in a form that allows identification of data subjects only for as long as necessary for the intended purpose of the collection.³³ Processing is permissible with the unambiguous consent of the data subject or if it is “necessary for the performance of a contract” with the subject or for the fulfillment of a legal obligation of the data processor.³⁴ Processing without consent is also permissible “to protect the vital interests of the data subject”;³⁵ this provision permits processing of an individual’s data for purposes of giving health care in an emergency, for example. Consent is also not required for tasks “carried out in the public interest” or for tasks carried out “in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.”³⁶ These provisions permit data processing for authorized public health purposes.

An important feature of the Directive is the special protections it provides for categories of especially sensitive information. These categories include “data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership . . . health or sex life.”³⁷ For data in these categories, the subject’s explicit consent to processing is required, with certain exceptions.³⁸ One relevant exception is that member states may prohibit processing of sensitive data even with the subject’s consent.³⁹ Processing of sensitive data may be permitted without consent if the “processing is necessary to protect the vital interests of the data subject or of another person” or the data subject is incapable of giving consent.⁴⁰ An example would be a public health authority processing information needed to trace contacts of an Ebola patient where the patient is unable to give consent. In addition, these special strictures on the processing of sensitive data do not apply to processing by health care providers under national

²⁹ *Id.* art. 3(2), at 39.

³⁰ *Id.*

³¹ *Id.* art. 9, at 41.

³² *Id.* art. 6(1)(b), at 40.

³³ *Id.* art. (6)(1)(e).

³⁴ *Id.* art. 7(a)–(c).

³⁵ *Id.* art. 7(d).

³⁶ *Id.* art. 7(e).

³⁷ *Id.* art. 8(1).

³⁸ *Id.* art. 8(2)(a).

³⁹ *Id.*

⁴⁰ *Id.* art. 8(2)(c).

law “for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services.”⁴¹

A further provision of Directive 95/46/EC allows member states to create special rules for the processing of data for scientific research. Although data subjects have rights to information about whether data about them are being processed and to request correction of processing that is not in accord with Directive requirements,⁴² member states may restrict these rights in the case of scientific research.⁴³ Restrictions require adequate legal safeguards, including that the data not be used for decisions regarding particular individuals and that the privacy of the data subject be protected.⁴⁴

Directive 95/46/EC also prohibits the transfer of data outside of the EU to any jurisdiction that does not meet the EU's standards for an adequate level of protection.⁴⁵ Because of the vast differences between their data protections, concerns arose that the EU would consider US protections inadequate and thus that it would be difficult to transmit data from the EU to the US. The solution has been the establishment of a “safe harbor” by the US Department of Commerce. Under the “safe harbor,” an entity receiving data from the EU may self-certify that it will process data according to EU standards.⁴⁶ Failure to honor this certification is considered a deceptive trade practice, subject to enforcement action by the Federal Trade Commission (FTC).⁴⁷

An additional area of tension in data policy between the EU and the US is data transfers for law enforcement purposes. These transfers are outside of the scope of Directive 95/46/EC. Since 2011, however, the EU and the US have been negotiating an agreement to permit the flow of data for national security and law enforcement purposes. In the aftermath of the revelations of the US PRISM program, these negotiations continue to be stalled. A particular area that remains unresolved concerns the rights of EU citizens to seek judicial redress for treatment of their data in the US. For example, a EU citizen who has been erroneously identified as a security risk might have data transferred to the US and then be denied entry. That EU citizen would have rights to have the data corrected in the EU, and it is the EU's position that the same rights should apply for the EU citizen to seek correction in the US.⁴⁸

⁴¹ *Id.* art. 8(3), at 41.

⁴² *See id.* art. 12, at 42.

⁴³ *Id.* art. 13(2).

⁴⁴ *Id.*

⁴⁵ *Id.* art. 25, at 45–46. For exceptions to this parallel exception to the requirement of consent for data processing, see *id.* art. 26, at 46.

⁴⁶ U.S. Dep't of Commerce, *Welcome to the U.S.-EU Safe Harbor*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018365.asp (last updated Apr. 11, 2012, 2:19 PM).

⁴⁷ U.S. Dep't of Commerce, *U.S.-EU Safe Harbor Overview*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018476.asp (last updated Dec. 18, 2013, 3:45 PM). See 15 U.S.C. § 45 (2012), for the section of the Federal Trade Commission Act that prohibits unfair and deceptive trade practices.

⁴⁸ *Factsheet EU-US: Negotiations on Data Protection*, EUR. COMMISSION (June 2014), http://ec.europa.eu/justice/data-protection/files/factsheets/umbrella_factsheet_en.pdf.

In the years since the implementation of Directive 95/46/EC, technology has changed enormously. At the time of the Directive's implementation, social networking, cloud computing, and crowd sourcing had not been developed, and even email was far different than it is today. The "internet of things"—smart devices—is increasingly apparent.⁴⁹ Other problems with Directive 95/46/EC have also become increasingly apparent, including significant variations in implementation among member states, confusion about the identification of data controllers and processors, and tensions over the adequacy of the EU-US safe harbor.

As a result, and after extensive study beginning in 2009, the EU has undertaken to reform the Directive.⁵⁰ The reforms were proposed by the European Commission in 2012 and adopted by a vote of the European Parliament in the spring of 2014.⁵¹ They await final approval by the European Council of Ministers.⁵² There are some concerns that the approval process has stalled, however, and France has recently urged strengthening plans for adoption.⁵³ These proposed reforms make many procedural and substantive changes that are relevant to health information.

An initial procedural change is that the proposed reforms take the form of a regulation rather than a directive. This means that member states will have less flexibility than they currently enjoy in their implementation of Directive 95/46 and thus there will be more uniform data protection rules across the EU.⁵⁴ An important constraint does remain in that the principle of subsidiarity must continue to be met. Importantly, the new EU regulation clearly will apply to any company doing business within the EU, even if the data processing is actually performed elsewhere, as with cloud storage.⁵⁵

New substantive requirements include the implementation of reasonable technical measures and organizational procedures for privacy by design.⁵⁶ Measures

⁴⁹ Article 29 Data Protection Working Party, *supra* note 9, at 3–5. Many of these devices process health information. Because the information is personally identifiable, it falls within the purview of Directive 95/46/EC. *Id.*

⁵⁰ See *Why Do We Need an EU Data Protection Reform?*, EUR. COMMISSION, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf (last visited Jan. 26, 2015); see also Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM (2012) 11 final (Jan. 25, 2012), http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [hereinafter Proposed Data Protection Regulation].

⁵¹ See General Data Protection Regulation, *supra* note 50; see also Press Release, European Comm'n, Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote (Mar. 12, 2014), http://europa.eu/rapid/press-release_MEMO-14-186_en.htm.

⁵² Press Release, European Comm'n, *supra* note 51.

⁵³ *EU Urged to Enact Stalled Data Protection Laws as France Proposes New Measures*, OUT-LAW.COM (Sept. 23, 2014), <http://www.out-law.com/en/articles/2014/september/eu-urged-to-enact-stalled-data-protection-laws-as-france-proposes-new-measures/>.

⁵⁴ See *Monitoring the Application of Union Law*, EUR. COMMISSION, http://ec.europa.eu/eu_law/introduction/what_directive_en.htm (last updated Sept. 12, 2014).

⁵⁵ See Proposed Data Protection Regulation, *supra* note 50, art. 3(2), at 41.

⁵⁶ *Id.* art. 23, at 56.

such as privacy-protective default settings would be required. The proposed Regulation stipulates that the data controller bears the burden of proving the data subject's consent to processing for specific purposes; consent must be presented in a manner that is distinguishable from any other written materials provided along with it.⁵⁷

Another quite high-profile substantive change is the inclusion of the "right to be forgotten" in the Regulation.⁵⁸ A version of this right was applied by the European Court of Justice in its 2014 decision involving the Spanish data protection authority's request that Google eliminate links in a search for a private citizen's name to a newspaper's publication of a record of his long-ago resolved debt.⁵⁹ Implementation of this decision remains controversial, however. Search engines such as Google have posted forms for individuals to use to request erasure, which is really delisting the links from the search rather than full erasure of the data.⁶⁰ Google reported over 150,000 requests by the fall of 2014, of which it granted 41.6%.⁶¹ News organizations such as the BBC have in response decided to publish a continually updated list of all granted requests, asserting that some of the articles have been wrongfully removed and the public's right to know compromised as a result.⁶²

Personal data concerning health information command a separate article in the Regulation. Under Article 81, the processing of personal health data must be necessary for one of the following reasons:

(a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies; or

(b) reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices; or

(c) other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system.⁶³

⁵⁷ *Id.* art. 7(1)–(2), at 45.

⁵⁸ *Id.* art. 17, at 52–53.

⁵⁹ Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)* (E.C.J. May 13, 2014), http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065.

⁶⁰ *Search Removal Request Under Data Protection Law in Europe*, GOOGLE, https://support.google.com/legal/contact/lr_eudpa?product=websearch (last visited Jan. 26, 2015).

⁶¹ *Transparency Report: European Privacy Requests for Search Removals*, GOOGLE, <http://www.google.com/transparencyreport/removals/europeprivacy/> (last visited Jan. 26, 2015).

⁶² Dave Lee, *BBC to Publish 'Right to be Forgotten' Removals List*, BBC NEWS (Oct. 17, 2014), <http://www.bbc.com/news/technology-29658085>.

⁶³ Proposed Data Protection Regulation, *supra* note 50, art. 81(1)(a)–(c), at 95.

The Regulation also makes explicit that processing of personal data for historical, statistical, or scientific research purposes is lawful, subject to specified conditions and safeguards found in Article 83.⁶⁴ Under these Article 83 safeguards, personal data may be processed only if these research purposes cannot be otherwise fulfilled by processing data that does not permit, or no longer permits, the identification of the data subject.⁶⁵ The safeguards also include separation of identifiers to the extent that research purposes permit.⁶⁶ Health information may be processed for historical, statistical or scientific research, subject to these safeguards; an example is the compilation of patient registries to improve diagnosis and treatment of specific conditions.⁶⁷

Finally, the Regulation codifies the right to be forgotten and to erasure.⁶⁸ The right applies when the data are no longer needed for their purpose, the data subject withdraws consent and there is no other legal basis for processing, the data subject objects to the use of the information for marketing, or the data processing violates the regulation in some other way.⁶⁹ This right does not apply to the processing of data for historical, statistical, or scientific research in accord with the Regulation.⁷⁰

As approval for the proposed new Regulation has proceeded, some research and public health entities have voiced significant interpretive concerns. One concern is the likely scope of the public interest exceptions, especially for biomedical and public health research.⁷¹ Another concern is that if the Regulation is interpreted narrowly, it may hamper efforts to monitor population health.⁷² Still another concern is that increased harmonization—one of the goals of the reform—will undermine more effective data protection regimes already in place in some EU member states, especially Scandinavian countries.⁷³

Another important area of discussion about the new Regulation will be its impact on transfers of data between the EU and the US. The Regulation makes clear the importance of ensuring that transfers beyond the EU are to jurisdictions that meet EU standards.⁷⁴ There are calls within the EU for reconsideration of the

⁶⁴ *Id.* art. 6(2), at 44.

⁶⁵ *Id.* art. 83(1)(a), at 96.

⁶⁶ *Id.* art. 83(1)(b).

⁶⁷ *Id.* art. 81(2), at 95.

⁶⁸ *Id.* art. 17, at 51.

⁶⁹ *Id.* art. 17(1).

⁷⁰ *Id.* art. 17(2)(c).

⁷¹ See, e.g., Yves Coppieters & Alain Leveque, *Ethics, privacy and the legal framework governing medical data: opportunities or threats for biomedical and public health research*, 71 ARCHIVES OF PUB. HEALTH, no. 15, 2013, at 1; M. Stenbeck & P. Allebeck, "Do the planned changes to European data protection threaten or facilitate important health research?" *Eur J Public Health* 2011, 21(6): 682-3.

⁷² Carinci F, Di Iorio CT, Ricciardi W, Klazinga N, Verschuuren M. "Revision of the European Data Protection Directive: opportunity or threat for public health monitoring?" *Eur J Public Health* 2011, 21(6): 684-5.

⁷³ Hakulinen T, Arbyn M, Brewster DH, Coebergh JW, Coleman MP, Crocetti E, Forman D, Gissler M, Katalinic A, Luostarinen T, Pukkala E, Rahu M, Storm H, Sund R, Törnberg S, Tryggvadottir L. "Harmonization may be counterproductive—at least for parts of Europe where public health research operates effectively." *Eur J Public Health* 2011, 21(6): 686-7.

⁷⁴ Proposed Data Protection Regulation, *supra* note 50, arts. 40–42, at 69–71

US-EU safe harbor doctrine in the aftermath of Wikileaks. Indeed, the Commissioner-designate for the Digital Internal Market, Andrus Ansip, recently stated, "Safe Harbour is not secure. The Agreement has yet to live up to its name."⁷⁵ Ansip also asserted in the hearing that unless the US provides more specific conditions in its escape clause for national security, the EU should consider suspending the Safe Harbour Agreement.⁷⁶

III. DATA PROTECTION LAW IN THE US

Data protection law in the US is far more fragmented than in the EU.⁷⁷ In the US, privacy protections differ based on the type of entity holding information, the type of information, and the jurisdiction.⁷⁸

Health information is subject to a wide variety of federal and state laws. The Privacy Act of 1974 protects identifiable information possessed by the federal government.⁷⁹ Federal law also provides some additional protections for special types of data such as census data⁸⁰ or certain statistical information.⁸¹ Information possessed by state governments comes under the protection of each state's privacy and freedom of information act laws. These laws may permit the disclosure of at least some identifiable information, as when a newspaper in southern Illinois sought cancer registry data to investigate allegations of a cancer cluster caused by exposure to environmental toxins.⁸²

The primary US statute governing health information possessed by health care providers and payers is the Health Insurance Portability and Accountability Act (HIPAA).⁸³ This statute also applies to business associates possessing identifiable health information under contract with the primary entities it covers, such as vendors of electronic medical records systems.⁸⁴ It does not, however, apply to the myriad forms of apps or internet sites possessing health information, from personal health record providers to fitness apps to social networking sites such as Facebook or search engines such as Google. These non-HIPAA covered entities are governed instead by the Federal Trade Commission (FTC) Act prohibition on unfair or

⁷⁵ *Ansip Threatens to Suspend Safe Harbour Data Agreement with US*, EURACTIV (Jan. 8, 2015, 3:45 PM), <http://www.euractiv.com/sections/innovation-enterprise/ansip-threatens-suspends-safe-harbour-data-agreement-us-308962>.

⁷⁶ *Id.*

⁷⁷ See Robert M. Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, 6 SOFTWARE L.J. 199, 238 (1993).

⁷⁸ See *id.*

⁷⁹ See 5 U.S.C. § 552a (2012).

⁸⁰ 13 U.S.C. § 9 (2012).

⁸¹ 44 U.S.C. § 3501 (2012).

⁸² *S. Illinoisan v. Ill. Dep't of Pub. Health*, 844 N.E.2d 1, 2–3 (Ill. 2006). Despite evidence of the possibility of re-identification of individuals because of the small numbers of affected individuals with particular cancers, the Illinois court held that the state's Freedom of Information Act required disclosure of the cancer registry information.

⁸³ Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 26, 29, and 42 U.S.C.).

⁸⁴ 45 C.F.R. § 164.504(e) (2014).

deceptive trade practices.⁸⁵ In recent years, the FTC has brought actions against both HIPAA-covered entities and non-HIPAA covered entities for violating this prohibition. Examples include the settlement involving CVS Caremark for improper disposal of prescription labels⁸⁶ and the recent action against LabMD for allowing sensitive health information to be exposed to a file-sharing network and to identity theft.⁸⁷

HIPAA, despite frequent assumptions to the contrary, was not primarily intended as an information protection statute. Its primary goals were to further the portability of health insurance and to streamline health insurance transactions. The Security Rule and the Privacy Rule implement HIPAA. The Privacy Rule is distinguishing between uses and disclosures of protected health information for which patient authorization is required and uses and disclosures that do not require authorization.⁸⁸ There is also a small category of types of uses and disclosures that require giving patients an opportunity to object, such as a listing of the names and room numbers of patients admitted to a hospital or the sharing of health information in the patient's presence with persons involved in the patient's care.⁸⁹

A major category of uses and disclosures that do not require patient authorization is treatment, payment, and health care operations (including quality improvement and analytics of cost-effectiveness).⁹⁰ Uses and disclosures for health care operations are subject to what is called the "minimum necessary" standard.⁹¹ This provision of HIPAA is somewhat parallel to the proposed EU Regulation Article 81's treatment of health information for health care, although it extends more broadly and does not explicitly contain the EU's confidentiality requirement.⁹²

A second category of uses and disclosures that are permissible without patient authorization is uses and disclosures for public health purposes as required by law.⁹³ Once information has been transferred to public health authorities under this category, it is no longer under HIPAA protections.⁹⁴ This requirement is the parallel to the proposed EU regulation Article 81's disclosure for public health surveillance.⁹⁵ The HIPAA provision, however, leaves open to state legislatures decisions about what uses and disclosures they will enact for public health purposes.

⁸⁵ See 15 U.S.C. § 45 (2012).

⁸⁶ Press Release, Fed. Trade Comm'n, CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays \$2.25 Million to Settle Allegations of HIPAA Violations (Feb. 18, 2009), <http://www.ftc.gov/news-events/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial>.

⁸⁷ Complaint at 3-5, LabMD, Inc., File No. 1023099 (Fed. Trade Comm'n Aug. 28, 2013) (No. 9357), available at <http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf>.

⁸⁸ 45 C.F.R. § 164.502(a) (2014).

⁸⁹ 45 C.F.R. § 164.510 (2014).

⁹⁰ 45 C.F.R. § 164.501, 506 (2014).

⁹¹ 45 C.F.R. § 164.502(b) (2014).

⁹² Proposed Data Protection Regulation, *supra* note 50, art. 81, at 95.

⁹³ 45 C.F.R. § 164.512 (2014).

⁹⁴ *Id.*

⁹⁵ See Proposed Data Protection Regulation, *supra* note 50, art. 81, at 95.

States may strike a variety of balances between the protection of individual privacy and access to information by the public. A particularly noteworthy example of a state striking the balance against privacy in favor of the public's right to know is Illinois. The Illinois Supreme Court required the disclosure of state cancer registry data with cell numbers sufficiently small (a diagnosis of neuroblastoma, together with the date of diagnosis and zip code of the patient's residence) so that re-identification was possible by an expert.⁹⁶ In reaching this conclusion, the Illinois Supreme Court interpreted the statutory language of its Freedom of Information Act, and found that "tends to lead to the identity of" referred to what ordinary individuals might be able to do and not to the abilities of technologically sophisticated experts.⁹⁷

HIPAA also allows the use or disclosure of protected health information for law enforcement purposes, a potentially open-ended provision not subject to the minimum necessary standard.⁹⁸ This provision also opens the possibility of extensive transfers of health information of the sort objected to by many in the EU after Wikileaks.⁹⁹

For research, HIPAA allows use of what is termed a limited data set of health information without patient authorization.¹⁰⁰ This is a data set that has been stripped of most identifiers, except some dates and locations;¹⁰¹ these data sets may permit more robust analyses than de-identified data, although they may not allow sufficiently accurate linking of records. HIPAA also permits the use of identifiable health information in research, if there is an Institutional Review Board or privacy board waiver of authorization based on a finding that the research could not practicably be carried out without the waiver and that patient privacy will be protected adequately.¹⁰² Otherwise, HIPAA requires patient authorization for the use of the health information that it covers in research. Tensions between these HIPAA requirements and the federal Common Rule used by many federal agencies to govern research with human subjects are notorious¹⁰³ and have led to proposals to amend the Common Rule.¹⁰⁴ These proposals have not as yet been acted on, however. In comparison to proposed EU Regulation Article 83's provisions governing use of health information for historical, statistical, or research purposes, these US requirements are impressively cumbersome.

⁹⁶ S. Illinoisan v. Ill. Dep't of Pub. Health, 844 N.E.2d 1, 18–21 (Ill. 2006).

⁹⁷ *Id.*

⁹⁸ 45 C.F.R. § 164.502(b), 512 (2014).

⁹⁹ See James D. Nordin et al., *Bioterrorism Surveillance and Privacy: Intersection of HIPAA, the Common Rule, and Public Health Law*, 98 AM. J. PUB. HEALTH 802, 804–06 (2008), for a proposal to integrate privacy protections in the use of health information for bioterrorism surveillance.

¹⁰⁰ 45 C.F.R. § 164.514(e)(1) (2014).

¹⁰¹ 45 C.F.R. § 164.514(e)(2) (2014).

¹⁰² 45 C.F.R. § 164.512(i) (2014).

¹⁰³ *E.g.*, INST. OF MED., BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 25 (2009).

¹⁰⁴ U.S. Dep't of Health & Human Servs., *ANPRM for Revision to Common Rule*, HHS.GOV, <http://www.hhs.gov/ohrp/humansubjects/anprm2011page.html> (last visited Nov. 23, 2014).

Like the EU, the US is thus considering at least some revisions to its regulatory structure governing the use of health information. However, consideration appears to be limited to the interplay between HIPAA and the federal regulations governing research with human subjects, at least at present. And it remains unclear if, or when, the Department of Health and Human Services will issue a notice of proposed rulemaking about revisions to the research rules; the advance notice was issued in 2011¹⁰⁵ and a notice of proposed rule-making had not been issued as of this Article's publication. Moreover, US privacy law is so fragmented in comparison with EU law, in terms of both jurisdictions and subject matter, that it appears unlikely that more comprehensive changes will occur at least in the next few years.

IV. CONCLUSION: TOWARDS MORE EFFECTIVE AND INTEGRATED USES OF DATA FOR HEALTH

Many important public health, health research, and treatment goals can be furthered by the use of health information. Privacy protection, as the EU recognizes, is an important aspect for facilitating the use and transfer of this information. All too often, privacy is seen as a barrier to information use, but without adequate assurances that data will be safeguarded appropriately, there are risks that data will not be shared at all.¹⁰⁶ Providing such assurances is a primary impetus for the EU's revision of its current data protection law.

As the EU moves towards adopting and implementing its proposed regulatory changes, it will be important to monitor the impacts on public health and medical research both within and beyond the borders of its member states. For the US, one concern will be whether the EU's increasingly stringent privacy protections will require revision of the safe harbor framework. There may also be growing divergence between the EU's overarching approach to the protection of personal information and the US's segmented approach that imposes very different restrictions on information within and outside of the HIPAA rules. Those interested in the responsible use of health information in the US might be well advised to watch how the EU's proposed Regulation plays out in the treatment of health information, especially the implementation of the provisions of Articles 81 and 83 governing the use of information for public health, improvement of health care, and medical research.

¹⁰⁵ *Id.*

¹⁰⁶ Letter from Larry A. Green, Chairman, Nat'l Comm. on Vital & Health Statistics, to Kathleen Sebelius, Sec'y, Dep't of Health & Human Servs. (Dec. 5, 2012), available at <http://www.ncvhs.hhs.gov/wp-content/uploads/2014/05/121205lt.pdf>.