Fordham International Law Journal

Volume 29, *Issue* 5 2005 *Article* 7

The Simplification of International Data Privacy Rules

Joel R. Reidenberg*

*

The Simplification of International Data Privacy Rules

Joel R. Reidenberg

Abstract

This Essay suggests that simplification will actually complicate data protection and will lead to unexpected burdens on industry along with an increase in the data surveillance of citizens. Part I begins with an examination of the global push for simplification. Part II addresses the opportunities for simplification through multiple instruments and some of the experiences with these instruments. Part III presents the obstacles to simplification. These obstacles illustrate fundamental problems with simplification. Part IV concludes with a proposal on "simplifying" technologies that calls for the development and increased use of privacy rights management technologies and technology audits to facilitate international data flows by simplifying the management of compliance across complex regulatory requirements and procedures.

ESSAYS

THE SIMPLIFICATION OF INTERNATIONAL DATA PRIVACY RULES

*Joel R. Reidenberg**

INTRODUCTION

The variation and complexity of national data privacy rules pose significant challenges for international data flows. Data protection laws range from ad hoc narrow legal rights, like those found in the United States, to comprehensive fair information practice statutes like those found in Europe.[1] Because data processing frequently occurs across national borders, multiple data protection laws might apply simultaneously to international data flows. At the same time, data protection regimes may prohibit the circumvention of national standards by processing personal information at a foreign site.[2] Global information processing thus presents a data controller with important burdens and obstacles related to compliance with varying standards and procedures.

One answer to this problem is the simplification of international data privacy rules. Proponents of simplification advocate reducing the burdens of compliance that come with the application of multiple data protection rules. While simplification can also arise in the national context itself, such as the short notice movement in the United States in connection with financial services,[3] for the global economy, proponents seek to facilitate international data flows.

---

* Professor of Law, Fordham University School of Law. An earlier version of this Essay was presented to the Twenty-Seventh International Conference of Data Protection Commissioners (Montreux, Switzerland, Sept. 14-16, 2005).

1. *See e.g.*, PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION 5 (1996).

2. *See* European Parliament and Council Directive No. 95/46/EC, art. 25, O.J. L 281/31, at 45-46 (1995) [hereinafter European Directive 95/46/EC] (on the protection of individuals with regard to the processing of personal data and on the free movement of such data).

3. *See* Interagency Proposal to Consider Alternative Forms of Privacy Notices Under the Gramm-Leach-Bliley Act, 68 Fed. Reg. 75164 (proposed Dec. 30, 2003) (to be codified at 12 C.F.R. pt. 40).

For simplification to be successful as a facilitator of international data flows, two critical conditions must be satisfied. First, an adequate level of privacy must be preserved. Second, the complexity and uncertainty of regulatory compliance must be reduced.

While these objectives are laudable, this Essay suggests that simplification will actually complicate data protection and will lead to unexpected burdens on industry along with an increase in the data surveillance of citizens. Part I begins with an examination of the global push for simplification. Part II addresses the opportunities for simplification through multiple instruments and some of the experiences with these instruments. Part III presents the obstacles to simplification. These obstacles illustrate fundamental problems with simplification. Part IV concludes with a proposal on "simplifying" technologies that calls for the development and increased use of privacy rights management technologies and technology audits to facilitate international data flows by simplifying the management of compliance across complex regulatory requirements and procedures.

I. *THE GLOBAL ECONOMIC PUSH FOR SIMPLIFICATION*

The transposition of the European Directive on data protection into Member State law,[4] the enlargement of the European Union ("EU"),[5] and the movement toward EU-style data protection in non-EU countries,[6] along with subnational rules—like the American data security law in California[7]—substantially increase the body of data protection law around the world. As online technologies mature, the sophistication of data processing techniques further increases the complexity of compliance with national data protection laws. On the Internet, interactive data collection and processing will typically target and involve computing resources in multiple jurisdictions. These contacts give

4. *See* European Directive 95/46/EC, art. 32, O.J. L 281/31, at 49-50 (1995). The directive provided for a transition period of three years for Member States to transpose the privacy standards into national law.

5. New Member States are required to have data protection laws that conform to European Directive 95/46/EC.

6. *See, e.g.*, Pablo Palazzi, La Transmisión Internacional de Datos Personales y la Protección de la Privacidad: Argentina, América Latina, Estados Unidos y la Unión Europea 39-41 (2002) (discussing the expansion of the European model to non-European countries).

7. *See* CAL. CIV. CODE §§ 1798.29, 1798.82 (2003).

States both the right and the obligation to assure data protection according to the local rules where those contacts occur—usually where the data subjects are located.[8] Similarly, Internet technologies give States new and enhanced powers to enforce their decisions online through electronic means. States can use electronic instruments such as packet interception, worms, and service attacks to sanction violators.[9]

When companies and government agencies seek to send or acquire data, the national differences in data protection regulation create significant compliance problems for those transfers. The multitude of applicable laws and regulations creates uncertainty for global businesses. Some data transfers may be impermissible under a country's rules because of conflicts related to the level of protection.[10] Other data transfers may be permissible, but more difficult to accomplish because of differences in standards such as consent requirements or formalities such as notification procedures.

Responsible multinational companies find this environment and the increasing complexity of managing compliance across multiple sets of data protection regulation confusing and potentially costly. This creates an incentive to seek simplified rules that are consistent across borders.

At the same time, governments now face similar concerns. Prior to the wave of Islamic terrorism over the last five years, the focus on international data transfers was global businesses. This emphasis has shifted to data transfers for security and law enforcement.[11] Government agencies seek personal data from foreign organizations that are subject to local data protection requirements. This often means that a multinational company can be caught in the middle between a request from a government where it does business and the obligations of data protection

---

8. *See* Joel R. Reidenberg, *Technology and Internet Jurisdiction*, 153 U. PA. L. REV. 1951 (2005). One should note that the interactive architecture of data processing will make the European Court of Justice's decision in the Lindqvist case obsolete. *See generally* Criminal Proceedings Against Bodil Lindqvist, C-101/01, [2003] E.C.R. I-12971, [2004] 1 C.M.L.R. 20.

9. *See* Joel R. Reidenberg, *States and Internet Enforcement*, 1 U. OTTAWA TECH. L.J. 213 (2004).

10. *See* European Directive 95/46/EC, art. 25, O.J. L 281/31, at 31 (1995).

11. *See* Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 6, ¶¶ 4, 37, 78-81 (2003).

regulations where it collects personal information. In these situations, government agencies seek to use a local organization as an intermediary agent to obtain data of foreign origin. The Passenger Name Record ("PNR") case[12] and the retention of electronic communications records[13] reflect this dilemma for industry. In the case of PNR, the U.S. Department of Homeland Security ("DHS") sought the transfer of passenger data originating from airlines in Europe to the U.S. Bureau of Customs and Border Control.[14] European regulators objected to the transfer.[15] By contrast, European data retention requirements may impose more stringent obligations on foreign communications service providers than the home countries of those providers. Governments, as a result, now also have an incentive to simplify data protection in order to facilitate international data flows for security and law enforcement.

II. *OPPORTUNITY THROUGH MULTIPLE MECHANISMS*

Various mechanisms offer opportunities to simplify data protection for the cross-border treatment of personal information. Instruments ranging from international law to technological infrastructure each might accomplish simplification tasks. However, experiences with most of these mechanisms raise questions for their success.

A. *International Law/Treaty*

International law provides the most obvious basis for simplification. The European Directive 95/46/EC[16] and Convention

12. *See* Agreement Between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, May 28, 2004, O.J. L 183/84 (2004) [hereinafter PNR Data Agreement].

13. *See* European Parliament and Council Directive No. 2006/24/EC, O.J. L 105/54 (2006), Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC.

14. *See* Council Decision No. 2004/496/EC, O.J. L 183/83 (2004).

15. *See, e.g.*, Working Party Opinion 2/2004 on the Adequate Protection of Professional Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection, 10019/04/EN, WP 87 (Jan. 29, 2004), *available at* http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp87_en.pdf.

16. *See generally* European Directive 95/46/EC, O.J. L 281/31 (1995) (protecting the right to privacy regarding the processing of personal data).

108 of the Council of Europe[17] each sought to create more unified, straightforward rules by comparison to the standards in place prior to the enactments. Further simplification, however, through international law is both unlikely and improbable in the short-term. Those instruments took years to implement.[18] More importantly, common procedures cannot exist effectively without an acceptance of common standards of protection. At the present time, common international standards and common international procedures are each elusive. In addition, commonly accepted protocols will not be sufficient. The implementation of common protocols will necessarily rely on other mechanisms.

B. *Legal Hybrids*

Data protection for international data flows may also be simplified through the use of legal hybrids. Legal hybrids are substitutes for specific regulations that prescribe common standards and procedures.[19] They attempt to give industry and government a non-statutory mechanism for compliance with divergent data protection standards. The principal impetus for legal hybrids came from Article 25 of the European Directive.[20]

1. Safe Harbor Agreement

The U.S.-EU Safe Harbor Agreement seeks to facilitate international data transfers between Europe and the United States and purports to assure compliance with European standards by organizations processing European data in the United States.[21] The mechanism is a legal hybrid because it anchors compliance in a set of policies that are not part of data protection legislation in the United States. The standards and enforcement mechanisms in the Safe Harbor streamlined those found in the European Directive.[22] While the Safe Harbor was an expedient effort

---

17. Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Europ. T.S. 108, *available at* http://conventions.coe.int/Treaty/enTreaties/Html/108.htm.

18. The European Directive was first proposed in 1990 and took five years for its completion.

19. *See* Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1332 (2000).

20. *See* European Directive 95/46/EC, art. 25, O.J. L 281/31, at 45-46 (1995).

21. *See generally* Commission Decision No. 2000/520/EC, arts. 1, 5, O.J. L 215/7, at 8-9 (2000) (setting forth safe-harbor framework).

22. María Veronica Pérez Asinari & Yves Poullet, *Privacy, Personal Data Protection*

to avoid confrontation between the United States and Europe, the mechanism has been ineffective. Both quantitatively and qualitatively, the implementation of Safe Harbor has been embarrassingly weak.[23] U.S. companies find the Safe Harbor process cumbersome while the resulting data protection is confused and often wholly insufficient. Since companies see a lack of resolve on the part of the European Union to enforce the European data protection regime, the use of Safe Harbor for compliance has few tangible incentives.

2. Contractual Arrangements

Contractual arrangements between companies are another important mechanism to solve compliance issues. Contractual mechanisms are a private law solution with limited public oversight. The model contracts approved by the Article 29 Working Party reflect this approach.[24] Companies wishing to use contractual arrangements to facilitate international data transfers can obtain the approval of European data protection supervisory authorities for their procedures. Contractual mechanisms, thus, provide companies with assurances of multi-jurisdictional compliance. However, the initial joint and several liability provisions of the model contract clauses sanctioned by the Article 29 Working Party have discouraged companies from using the standardized contracts.[25] Going forward, organizations are likely to seek variations on the model contracts that will reduce corporate obligations toward data subjects, and the Article 29 Working Party has recently shown some flexibility with respect to the joint and several liability provision.[26]

---

and the Safe Harbour Decision. From Euphoria to Policy: From Policy to Regulation. . . ?, *in* IN THE FUTURE OF TRANSATLANTIC ECONOMIC RELATIONS: CONTINUITY AMID DISCORD 101-134 (2005).

23. *See* Jan Dhont, María Veronica Pérez Asinari, Yves Poullet, Lee Bygrave & Joel R. Reidenberg, Safe Harbour Implementation Study 105-06 (2004), *available at* http://europa.eu.int/comm/justice_home/fsj/privacy/docs/studies/safe-harbour-2004_en.pdf; *see also* JOEL R. REIDENBERG & PRIVACY LAWS & BUSINESS, THE FUNCTIONING OF THE U.S.-EU SAFE HARBOR PRINCIPLES (Independent Consultant Study Report) (Sept. 21, 2001) (available from the European Commission).

24. *See* Commission Decision No. 2004/915/EC, O.J. L 385/74, at 75 (2004); *see also* Commission Decision No. 2001/497/EC, O.J. L 181/19, at 21 (2001).

25. *See* Commission Decision No. 2001/497/EC, Annex, Standard Contractual Clauses, cl. 6(2), O.J. L 181/19, at 26 (2001).

26. *See* Commission Decision No. 2004/915/EC, O.J. L 385/74, at 75 (2004).

3. Binding Corporate Rules

The most recent hybrid is the concept of "binding corporate rules." Multinational organizations may comply with European data protection requirements through binding corporate rules.[27] If the European data protection authorities approve an organization's internal rules and procedures, the private, internal corporate arrangement simplifies the task of satisfying local data protection obligations. As a very new instrument, there remains much uncertainty with respect to the minimum content of binding corporate rules and the enforceability of such rules. The pressure from multinational organizations is likely to push the level of data protection toward the lowest common denominator in the corporate family that is acceptable to European supervisory authorities. If successful, this effort will diminish the level of data protection as compared to European standards.

C. *Policy Instruments*

For security and law enforcement access to privately held personal information, simplification may occur through policy instruments at the inter-governmental level. The agreement between DHS and the European Commission for the transfer of passenger name record data from airlines in Europe to DHS illustrates this type of mechanism.[28] The PNR protocol is, in effect, a political rather than a legal instrument. The commitments are policy statements between governments that are not enforceable through the legal system.

D. *Technological Infrastructure*

The most significant hybrid mechanism to comply with varying data protection rules is the architecture of the technological infrastructure. Technological innovations move processing to multiple jurisdictions. While these innovations will often lead to multiple jurisdictional claims on data processing,[29] technological systems can arbitrate and automate compliance across different

27. *See* Article 29 Working Party, Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules, 05/EN, WP 108, at 2 (Apr. 14, 2005), *available at* http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp108_en.pdf.

28. *See* PNR Data Agreement, *supra* note 12.

29. *See, e.g.*, European Directive 95/46/EC, art. 4(c), O.J. L 281/31, at 39 (1995).

policy protocols. For example, compliance with multiple notification procedures can be automated as can multiple consent requirements and varying data subject access standards. Technological systems to incorporate multiple rules and procedures will not be simple to develop, but once developed can greatly facilitate international data flows.

Several recent cases illustrate the emergence of this mechanism. In the private sector, the P3P protocol and the movement toward multilayered notices in the United States and Canada demonstrate attempts to use infrastructure design as a way of accommodating different privacy policies.[30] Yet, some of these early efforts, namely P3P, have stalled on the incorporation of adequate privacy protections. In the security/law enforcement sphere, the negotiations between the U.S. DHS and the European Commission over access to passenger name record information also demonstrate the value of the design of the technological infrastructure to facilitate compliance. PNR access is to shift from a "pull" infrastructure where the U.S. authorities reach into European databases to a "push" infrastructure where the European data controllers would send data to the U.S. authorities. The more recent accord between Canada and the European Commission for the transfer of PNR data to Canada uses the "push" approach.[31] This design reduces concerns over compliance with data minimization standards and over foreign sovereign acts within local jurisdictions.

III. *OBSTACLES THROUGH VALUES CONFLICTS*

Data protection values will raise important obstacles to simplification. From the perspective of citizens, simplification necessarily reduces the precision of data protection and, in some jurisdictions, diminishes the level of privacy protection. This

30. P3P was designed as a technical standard that would allow users and web sites to agree on privacy policies for the treatment of personal data collected by the web site. *See generally* LORRIE FAITH CRANOR, WEB PRIVACY WITH P3P (2002). Similarly, the Ontario Information and Privacy Commissioner has advanced the use of layered privacy notices in the health care field. *See, e.g.*, Ann Cavoukian, Managing Your Legal Obligations Under PHIPA: Practical Advice and Best Practices in an Era of Privacy Transition (2005) (powerpoint presentation), http://www.ipc.on.ca/docs/2005-05-04-CanadianInstitute.ppt.

31. *See* Agreement on the Processing of Advance Passenger Information and Passenger Name Record Data, Mar. 21, 2006, E.C.-Can., art. 4, O.J. L 82/15 (2006) (requiring that data be "pushed" from airlines rather than "pulled" by Canadian authorities).

means that a primary goal of simplification—the preservation of an adequate level of privacy—will be quite difficult to achieve. From the perspective of industry, simplification has unintended consequences for security and law enforcement that may result in complex and costly procedures. This is counter to the second goal of simplification—the reduction in cumbersome procedures.

A. *Weakening of Data Protection*

Simplification inherently "dumbs down" or weakens data protection for some of the jurisdictions that have authority over the processing of personal information. An accord on common standards and protocols necessitates the abandonment of particular requirements adopted by national legislatures and regulators. The legal hybrids reflect this tendency. At the same time, the legal hybrids do not protect industry or citizens from public sector uses of privately held data.[32] Likewise, policy instruments are subject to strong inter-State pressures that may not protect citizens or industry. By contrast, technological infrastructures can go either way: they may provide weaker data protection through simplistic protocols or they may preserve data protection through more sophisticated, granular approaches.

Ironically, the inability of data systems to interconnect because of the complexity of regulatory compliance provides data subjects with privacy. Compliance difficulties reduce seamless data transfers and reduce the volume of data that may cross borders. In effect, personal information benefits from a "practical obscurity." Practical obscurity is the limitation on data collection and use that comes from a lack of standardization in processing. This means that standards such as purpose limitations and data minimization are enforced through practical barriers to data transfers. Simplification undermines this inherent protection.

By facilitating seamless data transfers, simplification inevitably encourages cross-border data mining and profiling. In combination with weakened standards, this effect can translate into remote surveillance activities by industry and law enforcement that are contrary to data protection values.

---

32. *See, e.g.*, USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

B. *Complicating Public Use of Private Data*

The shift in focus for simplification from the private sector needs to security and law enforcement purposes has important consequences for data protection. The data flows between the private and public sector mean that an increase in private sector transfers through simplification will correspondingly mean an increase in government desires to access privately held personal information across borders. As private sector transfers become more robust through simplification, law enforcement can use local organizations as the intermediaries for access to remote data. This will place industry in a difficult position. Law enforcement orders addressed to local organizations are mandatory and may be costly to manage. At the same time, such orders can undermine business relationships with trading partners and data subjects. In short, simplification for the private sector assists law enforcement in ways that may not be intended and in ways that escape traditional data protection.

IV. *PROPOSAL: "SIMPLIFYING" TECHNOLOGIES*

The opportunities and obstacles for simplification suggest that success will be very problematic for data protection and for industry. The multiple mechanisms themselves become complicated to manage as any organization may need to use more than one mechanism for the totality of its data processing activities. And, the mechanisms for simplification have important value challenges.

To facilitate international data transfers while respecting privacy, data protection can adapt a lesson from the intellectual property community. Intellectual property has "digital rights management" to secure copyright owners protection. Data protection should have "Privacy Rights Management" ("PRM") to secure the fair treatment of personal information. Like its intellectual property counterpart, PRM would package personal data with associated rights, obligations and procedures that are interpreted and effected through technological means. Instead of simplification that seeks to minimize compliance obligations, "simplifying technologies" should emphasize the development of the tools that robustly manage varying compliance procedures.

PRM technologies have two advantages for data protection and supervisory authorities. First, the development of PRM will

focus attention on the core policy decisions like the systems design issues did for the passenger name record case. Second, technological systems themselves can be audited more easily than data uses. Supervisory authorities can use automated tools to detect changes in the technology or technical configurations that impact on data protection.

Supervisory authorities should encourage the development of PRM technologies with an increased emphasis on participation in development projects whether by industry, standards bodies, or academic consortia. While this direction requires high level technical and legal expertise, it will be particularly useful to keep data protection functional in the global economy.

In the long term, however, policy and political differences underlying the regulatory complexity are likely to be resolved only through State-to-State compromises. PRM technologies will highlight the deep points of contention and will hopefully over time create conditions for an international legal instrument that is suited to interconnected global networks.