I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?

PAUL DE HERT & VAGELIS PAPAKONSTANTINOU*

Data privacy regulation has reached a crossroads: while three out of the four intergovernmental organizations that have released relevant regulations (the OECD, the Council of Europe, and the EU) are amending their respective texts, each one is implementing its own agenda. The Internet and cloud computing are making the need for international governance more evident than ever. Three scenarios may be foreseen: 1) the status quo remains, and technology intervenes to address public concerns; 2) the EU General Data Protection Regulation, which is expected to replace the EU Data Protection Directive by mid-2014, comes into effect and then goes on to set the international data privacy standard; or, 3) as suggested in this paper, an international data privacy organization, preferably a UN agency, is established to promote data privacy issues and warrant

* Paul de Hert is an international human rights expert. He teaches topics on international, European, and constitutional criminal law, legal theory, and human rights at the Vrije Universiteit Brussel. There, he also serves as Director of the VUB research group on Fundamental Rights and Constitutionalism, Director of the Department of Interdisciplinary Studies of Law, and a core member of the VUB research group, Law Science Technology & Society. He is also an associate professor at the Institute of Law and Technology at Tilburg University.

Vagelis Papakonstantinou is a partner in PKpartners Law Firm in Athens, Greece, as well as adjunct professor in the Department of Computer Engineering and Informatics at the University of Patras. He has extensive theoretical and practical experience in all fields of Information Technology Law and is the author of several books and articles with Greek and international publishers; he is also a regular speaker at national and international events, publishes regularly in the Greek press, has participated in several research projects at national and EU level and frequently consults the Greek government on related fields. He is also a Member of the Board of Directors of the Hellenic Copyright Organisation).

> international data privacy governance, similar to how the World Intellectual Property Organization advances the purposes of intellectual property protection. The establishment of an international organization does not necessarily mean that a new, comprehensive international data privacy framework also needs to be introduced (at least at this stage). Instead, international instruments already in effect could be used. The globally accepted but perhaps under-used 1990 UN Guidelines for the Regulation of Computerized Personal Data Files are an obvious choice.

Data privacy, since the appearance of the first relevant regulatory texts, may be listed among those few and relatively new fields of law that were developed across national borders. Within a single decade, beginning in the late 1960s, data privacy laws that implemented similar approaches appeared in several countries around the world. This informal transborder development was quickly followed by formal international instruments. In the early 1980s, when many countries that processed personal information had already introduced relevant legislation or were seriously considering doing so in the near future, international organizations entered the scene. The regulatory instruments they introduced attempted to converge the existing approaches that had, until that point, been implemented on the national level. These instruments became the common point of reference for subsequent new or amended national data privacy norms.

The international element that accompanied data privacy since its inception should be attributed—like the development of data protection as a separate field of law—to a single reason: the emergence of information technology. Until the late sixties, when the first data privacy laws were introduced, privacy issues were well identified (the now-famous Warren/Brandeis paper of 1890[1] was written when journalistic photography emerged) but did not lead to any specialized legislation on how to treat personal information. Instead, international treaties and only some national jurisdictions made reference to a general right to privacy. The exponential increase of the data processing ability computers provided to governments that could afford them necessitated the release of the first data privacy acts. The acts' provisions were aimed at regulating the way such automated and mass processing was to take place; a general reference to the right to

---

[1] Samuel D. Warren & Louis. D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

privacy was no longer considered sufficient to protect individual rights.

During the years that followed, data protection, (at least in Europe) developed, gaining, independence from its origins: the general right to privacy. However, the link between data privacy and information technology developments remained unbroken, and was actually further enforced. In fact, information technology developments form one of the two external factors, along with political developments, such as 9/11 and its aftermath, that set the international data privacy agenda.

Information technology converged with telecommunications, creating the current interconnected and internationalized environment of personal data processing, the Internet. Processing of personal information is no longer performed locally, or even within well-defined physical borders. The original "transborder flows of personal data,"[2] which by definition included transmission of data from one jurisdiction to another, were soon replaced by borderless continuous personal data processing, in which personal data are processed somewhere in the "cloud," that is, in indistinguishable server-farms installed around the world.

In addition, transborder personal data processing became individualized. Local data controllers are no longer needed to transmit their data subjects' data across borders to other data controllers in order for transborder exchanges to occur. Today, Web 2.0 applications enable individuals to upload their personal data to the "cloud," going to and from unidentified destinations.

Consequently, the need for international governance of data privacy is more important than ever. However, the means to achieve this still seem to be missing—or at least the ones at hand do not meet with the necessary international consensus.[3]

The first part of this paper will highlight the history of international governance of data privacy. It will also briefly describe the current state of governance to demonstrate that international norms followed data privacy legislation from the inception.

---

[2] *See* the title of the OECD data privacy instrument, "*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*."

[3] A necessary clarification at this point refers to the fact that, although the right to data protection is not the same as the right to privacy, and the terms "data privacy" and "information privacy" may have different content in different parts of the world, for the purposes of this paper these terms, unless otherwise stated, shall be used interchangeably.

International norms remain very much relevant today, through an exponential multiplication of sources.

The second part will elaborate upon the complexities of the contemporary processing environment by referring to two case studies, cloud computing and location-based services. These two examples will demonstrate that the transborder personal data flows model, as accommodated and implemented, has substantially changed in the past few years, at both the national and international level. Contemporary global and complex personal data processing makes international governance of data privacy more necessary than ever.

The third part of this paper elaborates upon the three plausible scenarios for the future. First, the *status quo* could remain. In this case, we suggest that technology will step in by offering technology-based solutions, such as Privacy By Design system architecture or Privacy Enhancing Technologies, to address the concerns of individuals about the best way to protect their private data. The second scenario considers the amendment process of the European data protection framework and the EU Data Protection Directive in particular. It predicts that an improved and updated version (likely in the form of the currently-developing EU General Data Protection Regulation) could constitute the international standard for data privacy either indirectly or directly, through streamlined application of its *adequacy* criterion. The third scenario recommended by the authors proposes the establishment of an international data privacy organization, preferably a UN agency, to govern international data privacy. The appropriate regulatory vehicle is perhaps already in place: the globally-accepted, but probably undeservedly underused, 1990 UN Guidelines for the Regulation of Computerized Personal Data Files. The field could also benefit from the examples of other sectors that achieved international governance status after decades of persistent efforts, despite the fact that they fostered similarly pervasive legislation, such as copyright.

THE PROLIFERATION OF INTERNATIONAL SOURCES OF PRIVACY NORMS

Today's proliferation of international sources of privacy norms was inevitable and anticipated since the first national data privacy laws were introduced. For the most part, this is probably due to the fact that information technology, demonstrated, since the beginning, disrespect for national borders, inciting the data privacy discussion and the first relevant laws. In this context, provisions on transborder exchanges of personal information may be found in the first national data privacy acts of the 1970s. The same is true for the *adequacy*

criterion which, as it will be demonstrated, permeates international data transfers today.

Apart from international elements in national data privacy acts, international organizations assisted the development of the data privacy field. During the 1960s and 1970s the OECD and the Council of Europe provided the necessary *fora* for the exchange of information among countries that processed personal data, contributing to the similarities evident in the first national data privacy acts. The same organizations further assisted data privacy development through the enactment of the first international, harmonizing, and influential instruments in the early 1980s, setting the basis for subsequent regulatory initiatives.

The years that followed only reinforced the need for international governance of data privacy. The Internet, in its various versions (1.0, 2.0 etc.), was the catalyst, limiting the ability of national regulators to adequately protect the individual right to information privacy.

Today, a multitude of supranational sources of data privacy norms exist, both at an international and at a regional level. These may be institutional or less formal and have variable legal statuses, scope, and substantive provisions. Together they comprise the contemporary international data privacy regulatory environment.

Despite the proliferation of international sources of data privacy norms, implementation remains local. In effect, depending on national restraints (for instance, participation or not in an international organization), it is up to national governments to decide whether to introduce data privacy legislation, which international model to apply (UN, OECD, Council of Europe, EU, or the Asia-Pacific Economic Cooperation (APEC)), how to implement it, and how to balance it against other human rights or other considerations (state security, finance, etc.). Therefore, for the time being, international governance of data privacy retains a horizontal character: it sets the agenda and formulates broad principles, but leaves the implementation at the local level. This regulatory model, as it will be demonstrated in Part II of this Paper, has reached its limits through contemporary Web 2.0 applications.

THE YEAR 1980: CRITICAL IN THE DEVELOPMENT OF INTERNATIONAL DATA PRIVACY GOVERNANCE

The year 1980 marked a critical moment in the development of data privacy norms. By that time the initial enthusiasm for the new field of law had subsided, with all interested countries. Austria, France, Germany (both at state and federal level), Sweden, and the

United States had already equipped themselves with relevant legislation. The rest of the countries performing data processing by automated means were, perhaps, reluctant to follow.[4]

Nevertheless, even at that time transborder flows of personal data were taking place at an increasing pace. International business cooperation became difficult; the need for some regulations on automated personal data processing was felt, but not everybody shared the same enthusiasm for the introduction of formal data privacy acts. [5] The institutional internationalization of the data protection law-making process became necessary to encourage and formalize a possibly broad adoption of the new field of law.

This section shall elaborate upon the first international sources of privacy norms that appeared in the early 1980s, the contribution of the international organizations concerned, as well as make brief reference to the international elements of the national data privacy acts in effect until that time.

THE ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT TAKING AN INTEREST IN DATA PRIVACY

The OECD was the first international organization to have dealt expressly with the data privacy issue.[6] Its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* were adopted in 1980.[6] The Guidelines remain in effect until today, an achievement not to be overlooked given the information technology revolution that has since occurred. Another achievement of the OECD Guidelines refers to the fact that in practice they are the only international instrument that has won the widest possible consensus from its membership with regard to its subject matter. To date, the Guidelines

---

[4] See particularly the case of the United Kingdom in COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 82 (Cornell Univ. Press 1992).

[5] For the case of the USA, for instance, see Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L. J. 913 (2009).

[6] Work in the OECD started in 1968. *See* Hans Peter Gassmann, 30 Years After: The Impact of the OECD Privacy Guidelines, Address at the OECD Joint Roundtable of the Committee for Information, Computer and Communications Policy (ICCP), and its Working Party on Information Security and Privacy (WPISP) in Paris, France (Mar. 10, 2010); COLIN J. BENNETT & CHARLES RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 88 (MIT Press 2d ed. 2006).

have been adopted by members representing such diverse approaches to data privacy as Germany, the United Kingdom, Canada, United States, Japan, and Korea.

The OECD has achieved such broad consensus on its Guidelines by purposefully focusing on the formulation of basic personal data processing principles that could be built into member country legislation, rather than detailing a model law to be incorporated as a whole[7]—a lesson of value today, as well (see below, III). It intently abstained from partisanship in the basic data privacy disputes raised at the time.[8] A key purpose of the Guidelines was to "advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries" they therefore intended to improve international cooperation rather than national law harmonization.[9]

The promise of international cooperation did not necessarily translate into international governance. The OECD Guidelines only set a voluntary, common basis for national regulation on data privacy, but did not create any permanent international mechanism for their implementation. In this context, their Part Five listed a series of recommendations to member countries (for instance, to make known among them details of their observance of the Guidelines, to introduce simple procedures for transborder data flows, etc.), which aimed to facilitate transnational information exchanges but from a national law point of view.[10] The Guidelines led members to consider data privacy at national level and respond to the need to protect individuals while also allowing for transborder data flows to take place, a self-restraint that proved wise over the years.

Because work toward the release of the Guidelines essentially coincided with initiatives in the Council of Europe (see below), cooperation between the two international organizations was formally

---

[7] *See* Michael Kirby, The History, Achievement, and Future of the 1980 OECD Guidelines on Privacy, Address at the Round Table on the 30th Anniversary of the OECD Guidelines on Privacy in Paris, France (Mar. 10, 2010); BENNETT, REGULATING PRIVACY 136.

[8] For instance, whether data privacy referred only to automated processing or how sensitive data should be processed, see OECD, *supra* note 7 art. 4 and Explanatory Memorandum.

[9] *See supra* note 7.

[10] *See* David Wright, Paul de Hert & Serge Gutwirth, *Are the OECD Guidelines at 30 Showing Their Age? Communications?*, 54 COMM. OF THE ACM, no. 2, 119-27 (Feb. 2011).

acknowledged:[11] The OECD perspective stated that, "during its work the Expert Group maintained close contacts with corresponding organs of the Council of Europe. Every effort was made to avoid unnecessary differences between the texts produced by the two organizations; thus, the set of basic principles of protection are in many respects similar."[12]

THE COUNCIL OF EUROPE PRODUCING A DATA PRIVACY CONVENTION IN 1981

A few months later, in early 1981, the Council of Europe introduced its Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).[13] The Convention was the first and still is the only legally binding international instrument in the data protection field: it requires its signatory states to apply its principles in their domestic legislation.

In the Council of Europe work in the data privacy field began as early as in 1968;[14] here again, the motivation lay expressly within advances in the information technology field.[15] The Convention included the Fair Information Principles and the special set of data protection rights for individuals (to information, access and rectification).[16] As far as international governance is concerned,

---

[11] *See* Kirby, *supra* note 7, at 8.

[12] OECD, *supra* note 7, at Explanatory Memorandum para. 20.

[13] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. 108 ("Convention 108").

[14] *See also* BENNETT, *supra* note 3, at 133; BENNETT & RAAB, THE GOVERNANCE OF PRIVACY, *supra* note 6, at 84. In practice, the cross border development of data privacy was realized through work in the OECD and the Council of Europe, as well as through "a closely knit group of experts in different countries [that] coalesced, shared ideas, and generated a general consensus about the best way to solve the problem of protecting the privacy of personal information." BENNETT & RAAB, THE GOVERNANCE OF PRIVACY, *supra* note 6, at 8, 112; *see also* Charles Raab & Bert-Jaap Koops, Privacy Actors, Performances and the Future of Privacy Protection, *in* REINVENTING DATA PROTECTION?, *supra* note 14, at 209 (Serge Gutwirth et al. eds., Springer Science 2009).

[15] *See* Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Explanatory Report, Jan. 28, 1981, E.T.S. 108.

[16] *See also* Paul de Hert & Eric Schreuders, The Relevance of Convention 108, Paper presented at the European Conference on Data Protection on Council of Europe Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data: Present and Future in Warsaw, Poland 34 (2001).

> having regard to the rapid evolution of information handling techniques and the development of international data traffic, it is desirable to create mechanisms at the international level which enable States to keep each other informed and to consult each other on matters of data protection.[17]

However, the mechanisms introduced by the Convention involve bilateral, intra-state cooperation and not the establishment of an international organization or committee authorized to deal with the relevant issues.

Most notably for the purposes of this Paper, the Convention was the first to formally establish the *adequacy* criterion for the exchange of personal data between two countries. In Article 12, the Convention allows local data protection authorities to refuse the transborder flow of personal data to countries that do not fulfill the criterion of having *adequate* data privacy legislation. The *adequacy* criterion was very much responsible for the expansion of data privacy legislation to those countries that hesitated in introducing it into their domestic law.[18]

As far as cooperation with other international or regional organizations is concerned, the Council of Europe, while working on its Convention, maintained a "close liaison" with the OECD "both at the Secretariat level and at the level of the Council of Europe's committee of experts and the corresponding OECD committee, the Data Bank Panel, which was succeeded in 1978 by an expert group on transborder data barriers."[19] Observer status was also granted, apart from the OECD, to Australia, Canada, Japan, and the United States. In addition, cooperation with the then-EEC was also formally secured.[20]

---

[17] Convention 108, *supra* note 13, at Explanatory Report, para. 11.

[18] Among which the most notable example is the United Kingdom, followed by the Netherlands, Australia and Japan. *See* BENNETT, *supra* note 3, at 143.

[19] OECD, *supra* note 6, at Explanatory Memorandum para. 20.

[20] *See id.* at para. 16.

A LATECOMER IN THE FIELD: THE UN GUIDELINES ON DATA PRIVACY OF 1990

The United Nations began work in the data privacy field in 1968.[21] Historically, the right to privacy was first expressly recognized in an international instrument in the text of the Universal Declaration of Human Rights of 1948 and the International Covenant on Civil and Political Rights of 1966.[22] Respectively, Articles 12 and 17.1 of these Conventions set forth that

> no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks" [23] and "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation.[24]

The UN turned its focus on the data privacy field, and specifically on "*computerized personal files,*" on September 11, 1980.[25] Work was

---

[21] UNITED NATIONS UNIVERSITY, HUMAN RIGHTS AND SCIENTIFIC AND TECHNOLOGICAL DEVELOPMENT Ch. 6 (UN Univ'y Press 1990), *available at* http://archive.unu.edu/unupress/unupbooks/uu06he/uu06he00.htm#Contents ("When its General Assembly, in its resolution 2450 (XXIII) of 19 December 1968, invited the Secretary-General . . . to undertake a study of the problems in connection with human rights arising from developments in science and technology, in particular from the following respects: a) Respect for the privacy of individuals . . . in the light of advances in recording or other techniques.").

[22] Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948), *available at* http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/043/88/IMG/NR004388.pdf?OpenElement; *see* International Covenant on Civil and Political Rights, Dec. 16, 1966, S. Treaty Doc. No. 95-20, 6 I.L.M. 368 (1967), 999 U.N.T.S. 171. The European Convention of Human Rights of 1950 also protected the right to privacy, in its Article 8. *See* European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 222.

[23] Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948), *available at* http://www.unhcr.org/refworld/docid/3ae6b3712c.html.

[24] International Covenant on Civil and Political Rights, Dec. 16, 1966, S. Treaty Doc. No. 95-20, 6 I.L.M. 368 (1967), 999 U.N.T.S. 171.

[25] *See supra* note 21.

carried out within the United Nations Human Rights Commission's Sub-Commission on Discrimination and Minorities. The first set of guidelines seems to have come out by 1983. Nevertheless, developments took place at an extremely slow pace (perhaps due to the fact that the issue, and any decision-making pertaining to it, was discussed during annual sessions within its respective Sub-Commission). Comments by member state governments took years to collect; the same is true for the completion of the various internal administrative steps before the issue was placed to the General Assembly for approval.

Therefore, it took the UN almost a decade to come up with its own Guidelines for the 1990 Regulation of Computerized Personal Data Files. [26] The Guidelines, although relevant only to automated processing, adopt the Fair Information Principles (Art. 1 – 7) as well as require that a local data privacy authority be established at national level (Art. 8).[27] For the protection of personal data, transborder data flows are allowed only between countries of "comparable" or "reciprocal" legal systems (Art. 9).[28] A less-noticed contribution to personal data privacy refers to the fact that the Guidelines, in their Part B, were the first to elaborate upon international organizations' data privacy, that is, the protection of personal information stored in the systems of international organizations. This seems to have taken several years to accomplish elsewhere.[29]

The UN Guidelines thus form an adequate data privacy regulatory framework, following the patterns and solutions that first appeared in the OECD Guidelines and in Convention 108. After all, the UN Guidelines belong to that first generation of international data privacy regulatory instruments, regardless of the fact that their elaboration took more than ten years to complete. This is an observation particularly important for the purposes of this Paper: developments at the UN level took perhaps an unnecessarily long time to complete, something that does not sit well with the contemporary pace of technological developments.

---

[26] UN Guidelines Concerning Computerized Personal Data Files, G.A. Res. 45/90, U.N. Doc. A/RES/45/90 (Dec. 14, 1990).

[27] *Id.*

[28] *Id.* at art. 9.

[29] For instance, the EU only introduced a European Data Protection Supervisor in 2001.

The UN Guidelines have received undeserved criticism for being of "limited practical relevance,"[30] mostly due to their non-legally binding character. This is probably exaggerated: the OECD Guidelines are non-binding, but there is a general consensus as to their global influence and central importance. Perhaps the root of such criticisms is related to the timing of the UN Guidelines. They came at a time, in 1990, when the OECD Guidelines and Convention 108 had already formed a concrete basis in the data privacy field, and the UN Guidelines did not offer much added value. Nevertheless, their greatest advantage was overlooked—even when compared with contemporary standards (that is, with the OECD Guidelines, the Convention 108, the Data Protection Directive, and the APEC Framework), the UN Guidelines address a vastly larger circle, placing them at a unique starting point for becoming the only truly international instrument for data privacy governance.

NATIONAL DATA PRIVACY DEVELOPMENTS UNTIL 1980

A basic characteristic of the first national data privacy laws was that they were developed across borders. Within only ten years of the appearance of the first data privacy act in the German federal state of Hesse in 1970, data privacy laws that implemented similar approaches made their appearance in several countries around the world.[31] The new field of law came expressly as the response to the emerging information technology and discussions on the surveillance societies,[32] regardless of the fact that both automated and manual processing were ultimately regulated by it. The policy options adopted in each national data privacy law, despite local differences as expected

---

[30] Christopher Kuner, *An International Legal Framework For Data Protection: Issues and Prospects*, 25 COMPUTER L. & SECURITY REV. 314 (2009).

[31] *See* Kirby, *supra* note 7, for the contention that "the nature of information technology and geographical proximity of the nations of Europe, as well as shared cultural, political, telecommunications and trade interests made the effort to secure harmony in legislation natural – and indeed inevitable" (referenced in BENNETT, REGULATING PRIVACY, *supra* note 3, at 139).

[32] *See* OECD, PRIVACY ONLINE: OECD GUIDANCE ON POLICY AND PRACTICE 11-14 (2003); BENNETT & RAAB, THE GOVERNANCE OF PRIVACY, *supra* note 6, at 126; DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 1 (UNC Press 1992); Burkard Eberlein & Abraham L Newman, *Escaping the International Governance Dilemma? Incorporated Transgovernmental Networks in the European Union*, 21 GOVERNANCE: AN INT'L J. OF POLICY, ADMINISTRATION & INSTITUTIONS, no. 1, 41 (2008).

among different legal systems, were substantially similar.[33] Points of consensus included the formulation of Fair Information Principles,[34] the granting to individuals of special data privacy related rights (information, access, rectification), or the establishment of dedicated controlling mechanisms for personal data processing. Another common concern among these first national data privacy laws referred to transborder data flows.

Germany was the first to see a data privacy law introduced at state level, and subsequently enacted its first Federal Data Protection Act in 1977.[35] At the time, although much attention was given to the introduction of a Federal Data Protection Commissioner, which would have to operate through a complex system of state, federal, public, and private administration,[36] the first German Data Privacy Act also expressly referred to transborder data flows introducing an early version of what later became known (see above, the analysis on the Council of Europe) as the *adequacy* criterion.[37]

France introduced its law on Informatics, Data Banks and Freedoms in 1978.[38] Here again, although significant attention was given to its regulatory model and the operation of the CNIL, the legislation placed a high priority on international cooperation: Article 1 of the legislation stated that "information technology should be at the service of every citizen. Its development shall take place in the

---

[33] *See* BENNETT, REGULATING PRIVACY 95 (quoting Frits Hondius & Justice Michael Kirby), as well as an OECD Report of 1975 (Developments in Data Protection and Privacy by OECD Countries).

[34] *See* BENNETT & RAAB, THE GOVERNANCE OF PRIVACY, *supra* note 6, at 12.

[35] German Federal Data Protection Act (BDSG), 1 Fed. Law Gazette 2814 (Jan. 27, 1977) (last amended Sept. 1, 2009).

[36] *See*, FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES, *supra* note 26, at 40; BENNETT, REGULATING PRIVACY, *supra* note 3, at 179.

[37] *See* BDSG, *supra* note 34, at §11; *see also* SPIROS SIMITIS ET AL., KOMMENTAR ZUM BUNDESDATENSCHUTZGESETZ (COMMENTARY ON BDSG), 390, 547 (Nomos 1978,). The same is also true for Sweden's first Data Protection Act, introduced in 1973. *See* Jon Bing, *Data Protection, Jurisdiction and the Choice of Law,* 1995 PRIVACY L. & POLICY REPORTER 65 (presented at the 21st International Conference on Privacy and Personal Data Protection *for* Office of the Privacy Commissioner for Personal Data in Hong Kong, China (1999)), *available at* http://www.austlii.edu.au/au/journals/PLPR/1999/65.html.

[38] Act No. 78-17 of January 1978 on Information Technology, Data Files, and Civil Liberties.

context of international cooperation."[39] Transborder data flows were also expressly and were regulated placed under the scrutiny of the CNIL.[40]

TODAY'S TRADITIONAL REGIONAL AND INTERNATIONAL SOURCES FOR DATA PRIVACY NORMS

The above sources of data privacy norms, established in the early 1980s, were soon joined by a number of others, both regional and international. Altogether, they now constitute the traditional, institutional international sources of data privacy norms.

As far as intergovernmental organizations are concerned, by now practically all of them with even a remote connection to data privacy have released relevant norms or at least some guidance. The central role of personal information to Internet business models has helped position data privacy close to the top of international agendas.

Similarly, norms created at the supra-national level may also be included in this category. This is the case, for instance, of supra-national courts or international advisory bodies, though they operate within different regulatory frameworks. Well-liked solutions or arguments released someplace in the world affect the responses to the same phenomena elsewhere due to the international character of data processing problems.

Although the relevant analysis exceeds the purposes of this paper, points of convergence among the international data privacy instruments discussed above include the Fair Information Principles or the granting of certain data privacy-specific rights to individuals (access, rectification, and redress). On the other hand, there is a point of divergence in regard to the controlling mechanisms. The formal establishment of institutional data protection authorities as an extra layer of public administration empowered to supervise data protection legislation locally is in contrast to other, less formal monitoring mechanisms that are either fully embedded in the administrative hierarchy or enjoy a certain level of autonomy.

---

[39] «L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale » (Information technology ought to be at the service of each citizen. Its development ought to take place within the international cooperation framework.).

[40] *See* Commission Nationale de l'Informatique et des Libertés (CNIL), Act No. 78-17; arts. 19, 24 (Jan. 1978) (on Information Technology, Data Files, and Civil Liberties).

In the thirty years after the release of the first international data privacy instruments, substantial work by the two organizations that released them (the OECD and the Council of Europe), as well as by newcomers (the UN, the EU, and the APEC), was undertaken regularly. They have added depth the field. In fact, each one of these organizations (with the disappointing exception of the UN) has created an impressive volume of work, both at the general principle-setting level and the sectorial case-specific level. Although this fact is encouraging and bodes well for the continued success of individual data privacy, one cannot help but note that these efforts are sometimes duplicative and largely advance in parallel. Because personal data processing issues are common globally (for instance, profiling, RFID, national security processing, etc.) position papers and norms produced by international organizations involved in the data privacy scene inevitably evolve around them. Although the regulatory framework that forms their basis of reference differs in each case, duplication of efforts and analyses frequently occurs.

On the other hand, missing from this framework is formal and institutional trans-organizational cooperation aimed at the formulation of a common regulative framework. Although certain international organizations enjoy privileged status at the bilateral level (for instance, the EU and the Council of Europe), the fact remains that, at most, an observer status is granted to representatives of other international organizations each time new data privacy norms are in the process of being introduced. Intra-organizational data privacy regulatory work remains, to date, more or less segregated, adding depth to the relevant basic instrument (for instance, the OECD Guidelines, the Convention 108, the EU Data Protection Directive, and APEC Privacy Framework) but creating common global data privacy models and principles.

CURRENT INTERNATIONAL AND REGIONAL DATA PRIVACY INITIATIVES (UN, OECD, COUNCIL OF EUROPE, APEC, AND EU)

The EU and the APEC were soon added to the above list of international organizations that first introduced data privacy norms (the OECD, the Council of Europe, and the UN). The EU continued to work rigorously in the field, adding depth to their regulatory instruments: the Guidelines and the Convention 108. APEC, despite the fact that it entered the scene with a delay of more than a decade, has demonstrated keen interest since. The influence of the EU is

particularly noteworthy, as its *adequacy* criterion [41] is probably responsible for the introduction of formal, institutional European-style data protection legal systems outside the EU.[42]

As far as the OECD is concerned, data privacy remained high on its agenda and substantial work has been undertaken on the basis of the Guidelines that continue to be in effect and unamended since 1980. The sectors that attracted the OECD's attention include critical information infrastructure, digital identity management, RFID, and privacy law enforcement cooperation.[43] However, the Guidelines have proved highly influential to the data privacy field, inspiring the enactment of relevant legislation in many regions around the world.[44] On their 30th anniversary, in 2010, the OECD has initiated discussions concerning their amendment and in 2011 it issued the relevant Terms of Reference.[45] The outcome of this process is still pending.

The Council of Europe furthered its Convention 108[46] through the 2001 release of an additional protocol regarding supervisory authorities and transborder data flows (significantly influenced by the EU Data Protection Directive), [47] as well as a series of recommendations and resolutions. A potentially significant development in international governance is the fact that the Council of

---

[41] Admittedly, the *adequacy* criterion is also to be found in Convention 108 (Art. 12) (Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. 108, art. 12) and in the UN Guidelines (*see supra* note 26, at art. 9). It is only the EU, however, that has actively implemented it in practice (see the relevant EU Commission webpages at http://ec.europa.eu/justice/policies/privacy/thirdcountries/index_en.htm (last visited Mar. 28, 2013)).

[42] *See also* Convention 108, *supra* note 40.

[43] *See* OECD, Directorate for Science, Technology and Industry, Information Security and Privacy Webpages, http://www.oecd.org/sti/privacyonlineoecdguidanceonpolicyandpractice.htm (last visited Mar. 28, 2013).

[44] *See* Kuner, *supra* note 24, at 314; Wright et al., *supra* note 9, at 119-27.

[45] OECD, Working Party on Information Security and Privacy, Terms of Reference for the Review of the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, OctoberPersonal Data (Oct. 31, 2011).

[46] The Convention celebrates its 30th anniversary in 2011; in this context, see the Council of Europe position paper on the Modernization of Convention 108, which was distributed at the 32nd International Conference of Data Protection and Privacy Commissioners in Jerusalem, Israel. Council of Europe, *Response to Privacy Challenges: Modernisation of Convention 108* (Oct. 27. 2010).

[47] *See* de Hert & Schreuders, *supra* note 16, at 43.

Europe opened up the ratification process of its Convention 108 to nonmembers. This supposedly will pave way for the Convention 108 to replace a still-missing international treaty on data privacy,[48] though with 38 countries having ratified the Convention to date, remarkable progress would be needed. The Council, almost at the same time as the OECD, began working on the amendment of its Convention 108, which was still an ongoing process in mid-2013.[49]

The EU entered the data privacy field relatively late, in 1995, but has perhaps dominated it since, at both a regional and international level. The main data privacy instrument it enacted is the EU Data Protection Directive.[50] The Data Protection Directive adopted the Fair Information Principles, affording individuals a set of inalienable rights (information, access, rectification) and introducing a formal, institutional mechanism for monitoring personal data processing in each Member State. International relevance was achieved through its *adequacy* criterion,[51] adopting a principle found in some of its Member States Data Protection Acts (and extending the relevant provisions in Convention 108). It requested that Member States export personal data only to third countries that warrant an *adequate* level of protection; such *adequacy* is to be determined centrally, by the European Commission (in its Article 25).[52] In this way, the EU has triggered the introduction of data privacy legislation to several third

---

[48] *See supra* note 38, at 108 ("Recognising that an international data protection framework has become crucial for the development and sustainability of democratic society and the effective exercise of fundamental rights and freedoms, the governments of member states of the Council of Europe called for accession to Convention 108 by states from all over the world with the required data protection legislation.").

[49] *See* Council of Europe, Final Document on the Modernisation of Convention 108, (T-PD (2012) 04rev - 17 Sept. 2012).

[50] Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 OJ (L 281/). The Data Protection Directive is currently in the process of review. *See A Comprehensive Approach on Personal Data Protection in the European Union*, COM (2010) 609 final (Apr. 4, 2010).

[51] *See* BENNETT& RAAB, *supra* note 6, at 95; Burkhard Eberlein & Abraham L. Newman, *Escaping the International Governance Dilemma?* 21 GOVERNANCE: INT'L J. POL'Y, ADMIN. & INSTITUTIONS 25, 40 (2008).

[52] The European Commission has released a list of countries that warrant such protection (only for commercial, pre-Lisbon Treaty First Pillar, personal data, a distinction that well exceeds the purposes of this paper), although after over ten years of implementation the list only comprises six countries.

countries that wish to do business with it. As will be later discussed (under III), the EU is also in the process of replacing its Data Protection Directive with a General Data Protection Regulation, expected to conclude by mid-2014.

APEC published its Privacy Framework in 2004.[53] The Framework consists of a set of nine principles that resemble the Fair Information Principles but sets a more flexible, lower standard for data privacy protection.[54] Its implementation by APEC member states is not mandatory. While implementing the APEC Privacy Framework would not necessarily meet the European *adequacy* criterion, the APEC framework is improving privacy protection standards in a region where such standards have been less common.

The UN, despite its unique position as a global and harmonizing player in the field, mostly kept clear from the data privacy field after the release of its Guidelines in 1990. Since 1990, the UN famously co-organized the World Summit on the Information Society,[55] whose agenda required it to establish a UN Group on the Information Society (UNGIS); its focus, however, seems to be oriented mostly towards facilitating developing countries' access to new technologies and promoting technology transfers.[56] The same is true for the UN's Commission on Science and Technology for Development and for the UN Human Rights Council. Data privacy is nowhere to be found in their agendas, despite the fact that data privacy matters were discussed in the 1970s and 1980s. It seems, therefore, that although the UN could play a central role in international data privacy governance, at the moment this is not an issue under consideration.

---

[53] The Asia Pacific Economic Cooperation, *APEC Privacy Framework,* (October 29, 2004), *available at* http://www.cyberlawcentre.org/ipp/apec_privacy_framework/APEC_Principles_local.htm. *See also* BENNETT& RAAB, *supra* note 6, at 104; Cecile de Terwangne, *Is a Global Data Protection Regulatory Model Possible?, in* REINVENTING DATA PROTECTION?, 175, 183-185 (Serge Gutwirth et al. eds.).

[54] *See* Graham Greenleaf , *Five Years of the APEC Privacy Framework: Failure or Promise?,* 25 COMP Law L. & SECURITY REV. 28, 37 (2009).

[55] *See World Summit on the Information Society,* INTERNATIONAL TELECOMMUNICATION UNION, http://www.itu.int/wsis/index.html (last visited Nov. 11, 2012).

[56] *See* UNGIS: UNITED NATIONS GROUP ON THE INFORMATION SOCIETY, http://www.ungis.org (last visited Nov. 11, 2012).

DATA PRIVACY IN RECENT NATIONAL LAWS AND CONSTITUTIONS

Over the past thirty years, data privacy laws have grown exponentially at the national level. Several countries have even added the right to data protection to their constitutions (for instance, Sweden, Belgium, Greece and the Netherlands). International governance undoubtedly played a major role in this development, both directly and indirectly. The OECD Guidelines, with the broad consensus they have achieved, have influenced many countries, including non-members, into introducing similar norms into their national legal systems. In addition, the *adequacy* criterion found in the text of the EU Data Protection Directive and the Council of Europe Convention 108 incited countries to introduce relevant legislation at national level.[57]

National implementations of data privacy norms vary considerably throughout the world, and the construction of a comprehensive list of the various approaches adopted to date falls beyond the purposes of this Paper.[58] Noted here is only the multitude of national approaches, which ultimately create an international data privacy regulatory patchwork.

Even within the EU, the European Commission has frequently had to intervene in order to ensure compliance, even though the EU Data Protection Directive has existed for over fifteen years and Member States harmonized their legal systems accordingly. In addition, the national security processing that was exempted from the scope of the Data Protection Directive; the ratification of the Lisbon Treaty that, among other changes, abolished the traditional pillar scheme; and sector-specific data protection regulations (ranging from PNR processing[59] to Schengen or Eurojust[60]), make the formulation of a

---

[57] On the extraterritorial effect of this criterion, see Yves Poullet, *Transborder Data Flows and Extraterritoriality: The European Position*, 2 J. INT'L. COM. L. & TECH. 141, 145 (2007). The *adequacy* criterion is by no means data protection (EU) particular; the United States uses the same principle in their Semiconductor Act 1984. *See* IAN J. LLOYD, INFORMATION TECHNOLOGY LAW 549 (2007).

[58] For more information, see Electronic Privacy Information Center's, *Privacy and Human Rights 2006–An International Survey of Privacy Laws and Developments* (EPIC 2006), http://www.epic.org.

[59] *See* Paul de Hert & Vagelis Papakonstantinou, *The EU PNR Framework Decision Proposal: Towards Completion of the PNR Processing Scene in Europe*, 26 COMPUTER L. & SECURITY REV. 368, 369 (2010).

[60] *See* Diana A. Blas, *The New Council Decision Strengthening the Role of Eurojust: Does It Also Strengthen Data Protection At Eurojust? in* DATA PROTECTION IN A PROFILED

single regional data privacy instrument extremely complex. These difficulties, however, are expected to be resolved once the new EU data protection framework comes into effect.

Outside of Europe, national approaches vary even more, ranging from European-like data privacy systems (in those countries that have passed the *adequacy* criterion[61]) to countries that apply a sectorial or a more flexible omnibus approach.

The various diverging data privacy regulatory schemes, entrenched in national administrative systems by several years of application, ultimately hinder the creation of a single international instrument for data privacy. Such a single, uniform regulatory instrument would need to re-draft or overhaul these approaches. Well-established procedures will have to be re-evaluated or abandoned. Additionally, data privacy regulations are often directed at powerful national data processing industries like the banking or insurance sectors, so legislative changes are frequently met with distrust. To survive, a single international instrument for data privacy must convince countries of the advantages of national implementation.

JUDICIAL AND ADVISORY OPINIONS ON INTERNATIONAL DATA PRIVACY GOVERNANCE

Most institutional international data privacy instruments established bodies with various roles (advisory bodies, secretariats, etc.) to implement their directives. In addition to these are the international bodies that were formed as a result of the international cooperation that proliferated since the first appearance of data privacy norms.[62] Finally, regional courts have often come to terms with data privacy norms in the exercise of their duties.

Within the EU, the Article 29 Working Party (of the EU Data Protection Directive) has become an important regional source of data

---

WORLD (Serge Gutwirth et al. eds., 2010); Paul de Hert et al., *Data Protection in the Third Pillar: Cautious Pessimism, in* CRIME, RIGHTS AND THE EU: THE FUTURE OF POLICE AND JUDICIAL COOPERATION 121, 128-30, 142-43 (Martin Maik ed., 2008).

[61] See the relevant list at the European Commission's website: *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries,* EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (last visited Nov. 11, 2012).

[62] *See* BENNETT& RAAB, *supra* note 6, at 144.

privacy norms.[63] Although its status is "advisory" and its mandate is to "make recommendations" or to "examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures," the Article 29 Working Party has produced an impressive volume of work and its legal opinions on data privacy challenges are closely observed by national Data Protection Authorities of Member States (whose representatives formulate the Article 29 Working Party). In addition, the European Data Protection Supervisor has also become an important regional source of data privacy norms, although mandated to function in a consultatory capacity and monitor data processing only within EU organizations.[64]

Apart from international bodies established by international data privacy instruments, the international cooperation in the data privacy field, since its inception, has led to the creation of less formal but perhaps equally important sources of norms. One such example is the International Conference of Data Protection and Privacy Commissioners (in 2010, already in its 32nd year).[65] The Conference, an annual forum[66] of data privacy exchanges from all over the world, has proved to be an important source of data privacy developments. It is a direct source through the common standpoints adopted towards common processing problems. The Conference is also the birthplace of other important internationalization initiatives, such as the Montreux Declaration (agreed by the Conference of 2005) and the Spanish Data Protection Commissioner's initiative for the creation of international standards for data privacy (connected to the Conference of 2009).

---

[63] *See* EBERLEIN & NEWMAN, *supra* note 42, at 40.

[64] See its incorporation mandate in European Parliament and Council Regulation 45/2001 on the Protection of Individuals With Regard to the Processing of Personal Data by the Community Bodies and on the Free Movement of Such Data, Dec. 18, 2000, 2001 O.J. L 8, 1 (EC).

[65] *See id.*

[66] The Conference may also be seen as a legal body. In 2009 it obtained observer status with the T-PD consultative committee. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Council of Europe, E.T.S. 108. Observer status to the Conference is in turn granted to the United States Federal Trade Commission and the United States Department of Homeland Security Privacy Office, among others. *See also* Charles Raab & Bert-Jaap Koops, *Privacy Actors, Performances and the Future of Privacy Protection*, *in* REINVENTING DATA PROTECTION?, *supra* note 14, at 207, 211.

The Spanish Data Protection Commissioner's initiative particularly constitutes a hopeful attempt towards the creation of an international set of rules for data privacy. The "Madrid Declaration" was formally adopted by the 31st International Conference of Data Protection and Privacy Commissioners and composed of eighty data protection authorities from forty-two countries. Its text expressly avoids any connections to EU data protection, trying to meet maximum international consensus. In this context, it is based on existing principles and criteria while guaranteeing an adequate level of protection. The "Madrid Declaration" has so far attracted positive reviews from the Council of Europe and the EU, as well as from privacy officers of some of the largest global corporations, meanwhile Mexico seems to be using it as reference text while introducing its own data protection act.[67]

Regional courts, like the European Court of Justice and the European Court of Human Rights, often confront a wide range of data privacy issues. [68] Although they implement different legislative frameworks, their approach to data processing problems, apart from its binding effect for signatory countries, adds a substantial volume of case law to the European data protection model thereby enhancing its exportability to interested countries.

THE RECENT TURN IN DATA PRIVACY GOVERNANCE TOWARDS SOFT LAW AND SPECIFIC LEGAL INSTRUMENTS: FIVE ILLUSTRATIONS

Contemporary practice has moved away from traditional institutional sources of data privacy governance, allowing other international sources of data privacy norms to gain importance.[69] These international sources stem from the need to make two different data privacy systems cooperate (for instance, the EU-USA Safe Harbor framework): the proliferation of *soft* law (codes of practice, ISO

---

[67] Information from Agustin Puente Escobar, Global and Implementable International Standards, Address Presented at the European Conference on Privacy and Data Protection in Budapest, Hungary (June 16-17, 2011).

[68] *See, e.g.*, Paul de Hert & Serge Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxembrourg: Constitualisation in Action*, *in* REINVENTING DATA PROTECTION?, *supra* note 44, at 3, 12-13, 16-23.

[69] *See* RAAB & KOOPS, *supra* note 14, at 209-12, 216;, 215ff, John Miller and David Hoffman, *Sponsoring Trust in Tomorrow's Technology: Towards a Global Digital Infrastructure Policy*, 1 INTERNATIONAL INT'L. DATA PRIVACY L.AW 83, 84, (2011), Vol.1 No.2, pp.83-91.

standards, trustmarks, etc.) as a preferred (mostly by the industry) alternative to formal regulation; and the introduction of data privacy norms into regulative texts of a different subject matter (for instance, in consumer protection laws, employment laws, spam laws, etc.).

Data privacy norms are not produced exclusively by state or public actors; they may also originate from the private sector. This development is in line with the broader phenomenon of new forms of international governance that blur traditional institutional regulatory mechanisms and create a complex, cosmopolitan environment.[70] These alternative sources of international data privacy norms enrich and expand the international framework for privacy protections, but complicate implementation for controllers and individuals alike.

INTERNATIONALLY DEVELOPED APPROACHES (FIRST ILLUSTRATION)

While data privacy legislation has an inherently cross-border dimension, its subsequent development inevitably acquired distinct national or regional characteristics. Perhaps most importantly, in European countries a new field of law emerged, data protection, which gained in depth and width and claimed its independence from the traditional right to privacy.[71] However, the European approach was not shared elsewhere in the world—perhaps most notably in the US Given, however, the globalization of transactions, as well as the national security imperatives, personal data need to travel across borders now more than ever. In order to accommodate the international cooperation of fundamentally different data privacy legal systems, a series of initiatives have been undertaken, particularly during the last decade.

The legal scheme implemented for the trans-Atlantic exchange of personal information is, in effect, a patchwork legal solution constructed on a limited, *ad hoc* basis. It includes the Safe Harbor Agreement[72] for commercial personal data exchanges, specialized agreements for PNR exchanges,[73] SWIFT exchanges,[74] and law

---

[70] *See* Henry Farrell, *Constructing the International Foundations of E-Commerce—The EU-US Safe Harbor Arrangement*, 57 INT'L ORGANIZATION, 277-78 (2003).

[71] *See* Stefano Rodota, *Data Protection as a Fundamental Right*, in REINVENTING DATA PROTECTION?; *supra* note 44, at 77-79.

[72] *See* BENNETT& RAAB, *supra* note 6, at 167; FARRELL, *supra* note 61, at 296-99.

[73] *See* Vagelis Papakonstantinou & Paul de Hert, *The PNR Agreement and Transatlantic Anti-Terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic*, 46 COMMON MKT. L. REV. 885 (2009).

enforcement data exchanges. On each side of the Atlantic, largely different provisions govern the respective processing once personal data have been transmitted. The resulting patchwork of data privacy regulations has led to the formulation of an informal advisory High Level Contact Group (HLCG) between the two parties in an attempt to facilitate bilateral cooperation at least in the law enforcement field.[75] The EU-US example is a powerful case for the advantages of introducing a single international data privacy instrument that would have saved both parties from a multitude of complex and hard-to-follow arrangements and, ultimately, a significant waste of resources in the respective negotiation and drafting processes.

Convergence among diverging national data privacy approaches is also attempted through internationally developed initiatives, such as the International Chamber of Commerce Task Force on Privacy and the Protection of Personal Data.[76] Among its objectives is the provision of assistance to businesses and governments, while allowing for flexible and effective global management of personal data. To this end, it has undertaken substantial work in the international transfers of personal data field. Additionally, the International Working Group on Data Protection in Telecommunications (the Berlin Group) was created in 1983 in the context of the International Conference of Data Protection and Privacy Commissioners[77] and has released a series of influential, at least at the EU level, working papers and resolutions within its subject-matter. Also, from the 1990s onward, the Hague Conference's Conventions and its implementing instruments has

---

[74]Paul de Hert et al., *SWIFT and the Vulnerability of Transatlantic Data Transfers*, 22 INT'L. REV. L, COMPUTERS & TECH. 191, 199 (2008).

[75] The Group submitted its final report in May 2008 (Council Note 9831/08, Final Report by EU-US High Level Contact Group on Information Sharing and Privacy and Personal Data Protection, final (May 28, 2008)); *see also* 275 S,Paul de Hert et al., *Are the OECD Guidelines at 30 Showing Their Age?*, 54 COMM. OF THE ACM, no. 2, 119, 123 (Feb. 2011).

[76] *See Privacy and Personal Data,* INTERNATIONAL CHAMBER OF COMMERCE, http://www.iccwbo.org/advocacy-codes-and-rules/areas-of-work/digital-economy/privacy-and-personal-data-protection (last visited Nov. 11, 2012) (ICC is the only business group awarded observer status in the Council of Europe T-PD Committee); Kuner C, Global Standards for Data Protection and Privacy: the Business Viewpoint, Presentation Address Presented at the European Conference on Privacy and Data Protection in Budapest, Hungary (June 16-17, 2011).

[77] *See also International Working Group on Data Protection in Telecommunications,* DATENSCHUTZ BERLIN, http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt (last accessed Nov. 11, 2012).

sought to ensure that international transfers of data occur in accordance with data protection obligations. [78] A more recent development is the Global Privacy Enforcement Network (GPEN),[79] "a network designed to facilitate cross-border cooperation in the enforcement of privacy laws."[80] GPEN was established in March 2010, in response to OECD's 2007 Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy. Among its tasks are the sharing of "*best practices in addressing cross-border challenges*" and the development of "*shared enforcement priorities.*"[81]

TECHNICAL STANDARDS: ISO INITIATIVES (SECOND ILLUSTRATION)

International technical[82] standards, despite the fact that they focus on the effectiveness of processes rather than an adequate level of (human rights) protection,[83] are of relevance to the international data privacy field.[84] Several relevant standards have been released for the evaluation of security methods of processing. By protecting information in computer systems, data privacy of the individuals concerned is also secured. In addition, consistent with the "code is law" [85] insight, the technical methods of application of such

---

[78] *See* Council on General Affairs and Policy of The Hague Conference on Private International Law Permanent Bureau, *Cross-Border Data Flows and Protection of Privacy*, Hague Conference on International Law (Mar. 2010), *available at* http://www.hcch.net/upload/wop/genaff2010pd13e.pdf.

[79] Global Privacy Enforcement Network, https://www.privacyenforcement.net (last visited Nov. 11, 2012).

[80] *Id.*

[81] *Id.*

[82] The various drafts of "Standards on Privacy and Personal Data," that are," released in the context of the Madrid Declaration, are not considered "technical" data privacy standards.

[83] *See* Jane K. Winn, *Technical Standards as Data Protection Regulation*, in REINVENTING DATA PROTECTION; *supra* note 44, at 191, 194.

[84] *See* BENNETT& RAAB, *supra* note 6, at 159.

[85] On the idea that "code is law", see LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (2000). On the data privacy extensions of this idea see BENNETT & RAAB, *supra* note 6, at 183; *see also* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 1 STAN. TECH. L. REV. 1 (2001), *available at* http://stlr.stanford.edu/STLR/Articles/01_STLR_1; Bert-Jaap Koops &

international standards supplement the data privacy norms that underlay them at a global level.[86]

In this context, the International Standards Organization has undertaken substantial efforts towards introducing data privacy or data privacy-related standards; its more than a dozen relevant standards vary from vertical data privacy-specific[87] and vertical data privacy-related[88] to horizontal privacy-related[89] texts.

Other organizations that have released technical data privacy standards of international application or influence include the Information Security Forum, [90] the European Committee for Standardization, and the British Standards Institution.[91]

SPECIFIC LEGAL INSTRUMENTS (THIRD ILLUSTRATION)

Data privacy norms may also be found among international and regional regulative instruments of different subject-matter; in these cases, the information privacy of individuals may occupy only certain provisions of an otherwise unrelated regulatory text or constitutes a secondary concern of lawmakers. [92] The EU Telecommunications

---

Ronald Leenes, *Code and the Slow Erosion of Privacy*, 12 MICH. TELECOMM. TECH. L. REV. 115 (2005), *available at* http://www.mttlr.org/voltwelve/koops&leenes.pdf.

[86] In this category should also be listed the various Privacy Enhancing Technologies (PETs) released from time to time (*see* Ari Schwartz, Looking Back at P3P: Lessons for the Future, Address presented at the Workshop on the Economic Benefits of PETs in Brussels, Belgium (Nov. 2009)).

[87] *See, e.g.*, ISO 22307:2008 on Financial Services: Privacy Impact Assessment.

[88] *See, e.g.*, ISO 9564-1:2002, Banking–PIN Management and Security–Part 1: Basic Principles and Requirements for Online PIN Handling in ATM and POS Systems.

[89] *See* ISO 18043:2006, Information Technology–Security Techniques–Selection, Deployment and Operations of Intrusion Detection Systems.

[90] *See The Standard of Good Practice for Information Security*, Information Security Forum (2003), *available at* http://www.netbotz.com/library/Info_Security_Forum_Standard_Good_Practices.pdf.

[91] *See* BS 7799-3:2006, Standard on Information Security Management Systems–Guidelines for Information Security Risk Management, *available at* http://www.iso.staratel.com/ISO17799/Doc/BS7799.3.1999/BS%207799-3-2006.pdf.

[92] Some speculation, not yet realized, also includes international trade law. Data privacy is frequently treated as a trade-related question (particularly with regard to international data transfers), so work within the WTO, and in particular the General Agreement on

(Electronic Communications) Framework: the ePrivacy Directive[93] is in its third version since its release in 1997 and constitutes an integral part of the EU Telecommunications Package. It is composed of seven instruments (six Directives and one Regulation) of regional effect.[94]

Intellectual property law has also been confronted with occasional data privacy issues. These cases confront the unlawful Internet exchanges of copyrighted material and the prosecution of such perpetrators. The proposed Anti-Counterfeiting Trade Agreement (ACTA) is a recent example of an international agreement that has data privacy implications.[95] The European Court of Justice has also been forced to balance the rights to data protection and intellectual property in its influential *Promusicae* case.[96]

Consumer protection regulations may also include data privacy norms as part of their protection of individual rights policy. For instance, the OECD, in its Guidelines for Consumer Protection in the Context of Electronic Commerce of 1999, included a section on privacy (in practice, referring to the OECD Privacy Guidelines) that aimed to ensure "appropriate and effective protection for consumers."[97]

Finally, anti-spam initiatives like the OECD Task Force on Spam issue recommendations for protecting individual privacy, although they do not place it at the top of their agendas.

Trade in Services (GATS), might at some point in the future be of relevance. *See* BENNETT & RAAB, *supra* note 6, at 108.

[93] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector O.J. 2002 (L 201) 37 (as amended by the 2009 EU Telecoms Reform).

[94] *See* Papakonstantinou & de Hert, *The Amended EU Law on Privacy and Electronic Communications after its 2011 Implementation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights*, 29 J. MARSHALL J. COMPUTER & INFO. L. FALL 29, 30, 38-39 (2011).

[95] *See* Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), OJ 2010 OJ. (C 147) 1.

[96] *Music Producers of Spain (Promusicae) v. Telefonica*, C-275/06 (Spain). See also, for instance, K Brimsted and G Chesney, "The ECJ's judgment in Promusicae: The unintended consequences – Music to the Ears of Copyright Owners or a Privacy Headache for the Future? A Comment," *Computer Law & Security Report* 2008, no. 24 (n.d.): 275-279.

[97] OECD, *Guidelines for Consumer Protection in the Context of Electronic Commerce* (1999), Part VII.

SELF-REGULATORY INITIATIVES AND TRUSTMARKS (FOURTH ILLUSTRATION)

The relationship between self-regulation and data privacy has always been tense and burdened with ambiguity. Self-regulation is interpreted differently than data privacy, and consequently they serve different roles in different parts of the world. While in the EU self-regulation is considered as a supplement to formal data privacy legislation, in third countries (particularly in the United States) outside a few sectors (e.g. financial and health) self-regulation has been considered an appropriate regulatory alternative to introducing and implementing strict data protection legislation.[98]

Self-regulatory initiatives normally originate from industry organizations of horizontal or vertical scope that wish to regulate their processing of personal data in order to gain public trust while also perhaps avoiding formal government intervention. In this context, initiatives such as the Global Business Dialogue on e-Society (GBDe) or the Online Privacy Alliance produce codes of practice, guidelines, etc., providing to their members concrete guidance as to how best deal with the processing of personal information in the course of their activities.[99]

Data privacy-related trustmarks (particularly web seals) constitute the practical extension of self-regulatory attempts. By affixing web seals onto Internet pages, members verify compliance to the data privacy standards and best practices more or less in the same way that notification of the processing to data protection authorities confirms its lawfulness in the EU. Indeed, such Internet trustmarks, or web seals, find extensive use outside Europe; in Japan, the PrivacyMark System has been in place since 1998 and has accredited more than twelve thousand private enterprises.[100] In the US, the first web seal program to come into existence was TRUSTe (originally Etrust) and was first used in an attempt to convince the EU on the *adequacy* of its data privacy protection model, and later used in negotiations for the

---

[98] *See* BENNETT & RAAB, *supra* note 6, at 152; Vagelis Papakonstantinou, *Self-Regulation and the Protection of Privacy*, 1st ed. (Baden-Baden: Nomos, 2002).

[99] GBD Home Page, http://www.gbd-e.org (last visited Nov. 11, 2012); Privacy Alliance Home Page http://www.privacyalliance.org (last visited Nov. 11, 2012).

[100] *See* Privacy Mark Home Page, http://privacymark.org (last visited Nov. 11, 2012).

conclusion of the Safe Harbor Agreement.[101] Another significant web seal initiative, equally US-based, includes the Better Business Bureau Online Privacy Program. Other web seal privacy-related programs are occasionally launched for the protection of individual privacy, with various penetration rates and effectiveness.[102]

INTERNAL CODES OF CONDUCT (FIFTH ILLUSTRATION)

A multitude of sector-specific codes of practice for the protection of individual data privacy, of various legal statuses and effectiveness, have been released by international and regional organizations from time to time. These codes of practice come in various formats and types.[103] They range from self-regulatory instruments of voluntary compliance without any monitoring or enforcement mechanisms, to strict sets of rules introduced in cooperation with state data protection authorities and even ratified by law in strict EU-like data protection systems.

Among them, perhaps the most significant are those released by international organizations in the course of exercising their duties: for instance, the International Labor Organization (ILO) has released its code of practice on workers' privacy, and the Federation of European Direct Marketing Associations (FEDMA) has introduced its own code on direct marketing.

Binding Corporate Rules (BCRs) should also be listed under this category. In effect, these are internal codes of practice adopted by multinational groups of companies and ratified by the competent national data protection authorities, which define the group's global data privacy policy with regard to the international transfers of personal data within the same corporate group to entities located in countries that may not provide an *adequate* level of protection, as per

---

[101] *See* H. Farrell, *Constructing the International Foundations of E-Commerce—The EU-US Safe Harbor Arrangement*, 278.

[102] Web Seals: A Review of Online Privacy Programs, a Joint Report of The Office of the Information and Privacy Commissioner/Ontario and The Office of the Federal Privacy Commissioner of Australia, 22nd International Conference on Privacy and Personal Data Protection, 2000, *available at* http://www.ipc.on.ca/images/resources/up-seals.pdf.

[103] *See* BENNETT & RAAB, *supra* note 6, at 155ff; Christopher Kuner, "Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future," *SSRN eLibrary* (October 1, 2010): 17, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1689483.

EU standards.[104] To this end, the extensive guidance provided by the Article 29 (EU Data Protection Directive) Working Party supplements the international framework for data privacy norms.

WORKING THROUGH THE IMPLICATIONS FOR CROSS-BORDER CONTROLLERS

The transborder personal data flows model accommodated in the several generations[105] of data privacy instruments, whether at the national or international level, has substantially changed in the past few years. This model was based on the existence of two basic assumptions, the first of which is knowledgeable, identifiable, and accountable data controllers, who exchange files of personal information across their corresponding jurisdictions; sometimes even the location of the server is of importance. Second is the local data protection authorities that are able to monitor and control the transmitting of personal information from their jurisdictions outwards.[106]

Both assumptions have been reversed. The Internet is the catalyst in its contemporary Web 2.0 format. As far as the notion of two data controllers in different jurisdictions exchanging files with personal data is concerned, today, individuals massively upload their own personal information (profiles) onto social networking websites located outside their jurisdiction. The location of the server criterion is thus less important when identifying the applicable national data privacy law, because processing takes place in indistinguishable server farms around the world. State authorities' local monitoring and control of all personal data exports is made impossible not only by the fact that state authorities are no longer notified of transborder data

---

[104] *See* the relevant EU Commission data protection webpages, *available a*t http://ec.europa.eu/justice/policies/privacy/binding_rules/index_en.htm.

[105] *See* Poullet, *About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?* in Gutwirth, Poullet, de Hert, *Data Protection in a Profiled World*, supra, 9-12 (2010). However, despite the generations past, controlling instances and processing models more or less correspond to those treated in the first data privacy laws of the 1970s.

[106] *See also* BENNETT & RAAB, *supra* note 6, at 269. For the broader protection of privacy scheme note that "according to the traditional paradigm, privacy protection entails an exercise of rights by Citizen A of Country A against an organisation that that was geographically located within Country A. These assumptions have obviously broken down[.]" *Id.*

transfers (because these are performed directly by individuals), but also by the fact that contemporary global players do not need to establish themselves in every country of the world anymore. Indeed, the prevalence of the Internet as a working medium, through cloud computing or other applications, means that local presence in different markets around the world is no longer necessary; operations can be run and services can be provided successfully from a distance. The lack of local subsidiaries further hinders local control by national data protection agencies.

One should not overlook other processing parameters as well. Widespread computing, the "Internet of things," and RFID promise continuous unobserved processing that will create vast amounts of personal data. These advances will render impractical the data controller/registration scheme for monitoring data processing within a state.[107]

Consequently, a complex personal data processing system emerges. It transcends both national borders and traditional models, marginalizing key players of the past and introducing new parameters for contemporary data controllers. In this context, traditional data privacy regulations, despite their international character, do not suffice. New tools and new methods should be devised to more efficiently regulate modern processing systems and traits.

The complexity of contemporary personal data processing will be more clearly demonstrated by reference to two case studies, cloud computing and location-based services. Each one disregards national borders and processing intermediaries, in the form of locally established data controllers, and is thus typical of contemporary data privacy implementation difficulties. They also seem to currently attract much public and financial interest, and are suggested as the two fundamental processing trends both for corporate and personal data processing—meaning that they are here to stay, at least for the foreseeable future.

---

[107] *See Data, Data Everywhere: A Special Report on Managing Information*, THE ECONOMIST, Feb. 27, 2010; Centre de Recherches Informatique et Droit (CRID), *Working Paper: Law Enforcement in the Clouds: Regulatory Challenges*, 1-2, 36-37 (2012), http://www.crid.be/cloudcomputing; Paul M. Schwartz, *Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment*, 10, 16-18 (2009), http://theprivacyprojects.org/wp-content/uploads/2009/08/The-Privacy-Projects-Paul-Schwartz-Global-Data-Flows-20093.pdf.

WHAT'S A CLOUD PROVIDER TO DO?

Cloud computing,[108] though by no means a new idea, seems to dominate the international processing environment today. The principle behind it is simple: individuals no longer need to maintain anything but the bare minimum of hardware (i.e., in their homes or offices). Instead, all one needs to work on files and execute processing on remote servers, often maintained by foreign companies, is access to the Internet, a screen, and a keyboard. The location of these servers is variable: they may reside anywhere in the world, depending on economies of scale, climate, and other considerations. They are installed in huge clusters, and it is conceivable that even their operators may have difficulty identifying which server performs which of their client's processing at any given moment. In other words, the main idea behind cloud computing is for individuals and companies to actually work on computer terminals and for the real processing to take place in outsourced, difficult-to-locate hardware.

This change begets new concerns because cloud computing, when regulating transborder data flows, undermines both assumptions of traditional data privacy law: accountable data controllers and competent local data protection authorities.[109] Data controllers in one country (assuming that cloud computing operators such as "Software as a Service"–SaaS providers are only data processors in the traditional data protection scheme) upload and store their data in the "cloud" and users located in other countries have access to the data by means of simply logging in, and not necessarily downloading personal information.[110] In this assumption distinction under data protection law, the between-data controllers, who are generally accountable, and data processors, who are normally not directly liable towards

---

[108] For example, EU Article 29 Data Protection Working Party, Opinion 5/2012 on Cloud Computing, (WP 196,) 2, 4 (July 1, 2012,); Lee Badger et al., *Cloud Computing Synopsis and Recommendations: Recommendations of the National Institute of Standards and Technology*, Special Publication 800-146, ES-1 (May 2011,); ENISA, *Cloud Computing: Benefits, Risks and Recommendations for Information Security*, Nov. 2009; *Let It Rise: A Special Report on Corporate IT*, THE ECONOMIST, Oct. 23, 2008; Le Monde Diplomatique, A'l ère de l' "informatique en nuages," in Internet, Révolution Culturelle, No. 109, Feb. – Mar. 2010 (France).

[109] Omer Tene, *Privacy: The New Generations International Data Privacy Law*, SSRNe Library 1-2 (2010), *available at* http://ssrn.com/abstract=1710688.

[110] *See* Article 29 Data Protection Working Party, *Opinion 1/2010 on the Concepts of "Controller" and "Processor"* 5-6 (Feb. 16, 2010).

individuals, is blurred.[111] In fact, even identifiable data controllers are no longer in a position to know exactly which international personal data transfers take place at any given moment within their systems.[112]

The role of data controllers is also weakened by the fact that cloud computing and Web 2.0 applications enable (or rather, expressly intend) for users to upload their personal information directly into the "cloud."[113] Once there, these data are accessible under various "privacy settings" to data controllers in the world to process. This consensual transfer of personal data across borders makes the transfer model, purportedly regulated by contemporary data privacy regimes, irrelevant.

On the other hand, local data protection authorities are at a loss if they wish to monitor the international data transfers originating from their respective countries. If in the course of their controlling duties they visit a data controller's premises, they will not find a server loaded with personal data and a trail of the international data flow. Rather, they will find computer terminals with access to the Internet where personal data is being uploaded. Security measures no longer need to be or can be observed, at least locally and nationally. Consequently, national regulations and requirements are hard to enforce effectively within such a processing environment.

Cloud computing not only creates difficulties for a personal privacy standpoint but also in terms of compliance. Data controllers who use cloud computing in their business and wish to observe data protection provisions will find it very problematic to make the appropriate notifications and receive the appropriate permits for their international data transfers. If they follow the "location of the server" principle, they cannot know exactly where their data is located and

---

[111] *See* Peter Hustinx, *Data Protection and Cloud Computing under EU Law*, European Parliament, 1-3 (Apr. 13, 2010), Janni Christoffersen, *Cloud Computing–A Challenge to Data Protection?*. Presentation during the International Data Protection Conference, Budapest, 20-21 (June 2011); Wojciech, Wiewiorowski, *Privacy and the Liability of Intermediary Service Provider in the Clouds: E-Governmental Aspects*, presentation during the International Data Protection Conference, Budapest, 1650, 52, 5416 (June 2011).

[112] Peter Hustinx, *Data Protection and Cloud Computing under EU Law*, European Parliament, 4 (Apr. 13, 2010)

[113] Peter Hustinx, *Data Protection and Cloud Computing under EU Law*, European Parliament, 5 (April 13, 2010); *see* Article 92 Data Protection Working Party, *The Future of Privacy: Joing Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data* (WP 168) (Dec. 01, 2009).

will therefore have to deal with multiple local regulators. Understandably, this will increase the resources and time required to acquire these permits. If they presume that the cloud-computing operator operates its servers at its home address, they risk having to follow legal requirements for international data transfers to countries that only provide facility headquarters, without any actual participation in the processing.[114]

Since 2001, and particularly after 9/11, a series of regulatory measures were undertaken around the world that would facilitate access to personal data for purposes of state security. All these measures are inevitably based on locality assumptions, meaning that local law enforcement authorities may access locally-held data to protect national security, while a complex web of data exchange regulations cater to international cooperation. The proliferation of cloud computing means that the information required for national security purposes will be even harder to trace, and this could lead to even more pervasive measures being undertaken, further eroding the general level of protection of individual privacy.

LOCATION-BASED SERVICES ON GLOBALLY AVAILABLE INTERNET PLATFORMS

Location-based services have thrived in the past few years, mostly due to a surge of public interest and the emergence of Web 2.0 applications.[115] Today, a wide range of Internet location-based services are available, all of which essentially refer to applications where users voluntarily feed in their location at different times during their daily routines in return for such location-relevant services.[116]

---

[114] Press Release, Article 29 Data Protection Working Party, European Data Protection Authorities Adopt Opinion on Cloud Computing (July 1, 2012); Legal Update, Mayer–Brown, Cloud Computing–Article 29 Working Party Guidance on EU Privacy and Security Concerns (July 2012). This is probably why the Art. 29 Data Protection Working Party strongly advises that "businesses and administrations wishing to use cloud computing should conduct, as a first step, a comprehensive and thorough risk analysis," ultimately, however, asking for data controllers to, self-voluntarily, opt for a "cloud provider that guarantees compliance with EU data protection legislation," admittedly not an easy task in contemporary complex global processing environment, where the most well-known global providers are located outside the EU.

[115] Applications that enable two-way communications between information providers and users (see in particular TIME 2006 Person of the Year–You, Dec. 25, 2006).

[116] The Art. 29 Data Protection Working Party distinguishes between "geolocation services that are available on and/or generated by smart mobile devices that can connect with the Internet and are equipped with location sensitive sensors such as GPS," which are

Telecommunications services should be viewed in the same category as companies that keep location data in their systems for prolonged periods of time for national security reasons. All these services are based on personal information; location-based data directly or indirectly pertains to an identifiable individual and constitutes. The uploading and processing of such data on the Internet and on Web 2.0 platforms or elsewhere most likely constitutes transborder exchanges of personal information regulated by data privacy laws.[117]

Regulatory limitations of national data privacy norms become immediately evident here as well.[118] From the users' ("data subjects") point of view, information is voluntarily uploaded to the Internet (in the "cloud") for further processing. It appears that users' consent to the processing, as required by basic (EU) data protection legislation,[119] is met in this fashion. However, most important are its particulars: individuals may upload their location-based data themselves, or permit it to be uploaded automatically through their electronic devices (like smartphones). In either case, data privacy laws require informed consent of individuals prior to the processing,[120] which is probably not satisfied by contemporary geolocation services models. The default "privacy settings" in devices or their social network websites may not always fulfill the requirement of informed consent needed by data privacy legislation. It is not always straightforward that a subsequent change of mind is warranted, meaning that the collected location-based data are actually going to be deleted from the data controllers'

---

subsequently elaborated in its Opinion 13/2011, and "geotagging technology linked to the so-called web 2.0 in which users integrate geo-referenced information on social networks such as Facebook or Twitter" or even "other geolocation technologies that are used to interconnect devices within a relatively small area (shopping centres, airports, office buildings, etc) such as Bluetooth, ZigBee, geofencing and WiFi based RFID tags." These distinctions demonstrate that the field remains under development and thus no clear lines may be drawn between services and providers.

[117] *See* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on The Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, 38 [hereinafter "Directive 95/46/EC"]; Article 29 Data Protection Working Party Opinion 13/2011 *on Geolocation Services on Smart Mobile Devices* (WP 185) 9 (May 16, 2011).

[118] *See* Tene, *Privacy: The New Generations*, International Data Privacy Law, 2010 SSRNe Library (2010), http://ssrn.com/abstract=1710688.

[119] *See* Directive 95/46/EC, *supra* note 117, at 40.

[120] Directive 95/46/EC, *supra note 117,* at 41-42 (on the individual right to information).

computer systems; this is a further breach of an important data protection principle: the individual right to rectification. [121] Geolocation personal data can be used for practically limitless and uncontrollable activities. The plurality of ways by which users may profit from location-based services (for instance, accessing promotional offers, finding friends who happen to be nearby, making new acquaintances, and accessing navigational information, etc.) is the basic incentive for making their personal information available to be processed by other parties.[122] However, the basic data protection principle of purpose specification of the processing is potentially breached.[123]

Internet-based geolocation services also contradict the controlling mechanism installed by contemporary data protection regimes. While personal information flows from the users' devices to server farms around the globe, it is automatic, continuous, and therefore practically uncontrollable by national data protection authorities.

On the other hand, state security authorities increasingly ask for access to location information of telecommunications subscribers to prevent crime and for national security purposes; in a globalized world, transborder requests are not infrequent.

As is the case with cloud computing, processing of location-based data creates common problems felt equally in different parts of the world. It also challenges the premises of the current data privacy legal scheme. Accountable, identifiable, local data controllers are the exception among today's providers of location based services; the competent local data privacy authorities that will monitor and control their processing are even harder to identify. Therefore, data privacy laws fail to effectively protect the individuals' right to data privacy for a substantial category of their personal information.

SOME CONCLUSIONS: COPING WITH COMPLEXITY

International governance has accompanied data privacy since the first relevant acts were introduced, and is very much in place today. However, in most cases, it occupies a horizontal character, shaping principles and setting the agenda, but not affecting implementation at

---

[121] *See* Directive 95/46/EC, *supra* note 117, at 42-43.

[122] *See also* US Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change–A Proposed Framework for Businesses and Policymakers, 23 (Dec. 2010).

[123] *See* Directive 95/46/EC, *supra* note 117, at 40.

national level (with the exception of the EU Data Protection Directive).

Even international sources of data privacy norms offer only partial convergence: the OECD data privacy model is more or less different than that of the Council of Europe and the UN, and, most starkly, that of the EU model. Although general consensus may be struck with regard to certain aspects of data privacy norms (for instance, on the Fair Information Processing Principles) this is not the case with other aspects of similar importance (for instance, the controlling mechanisms). Therefore, although international governance is well established, a single international data privacy regulatory framework is yet to be seen.[124]

On the other hand, contemporary data processing complexity makes anything but international governance for data privacy ineffective and even irrelevant.[125] Transborder data flows no longer take place in an organized way that is easy for state authorities to monitor, as prescribed in the data privacy laws in effect worldwide today. Instead, data controllers may reside anywhere in the world, data subjects upload their data directly onto their systems themselves, all for processing to take place in servers whose exact location is difficult to identify. This eradication of localized processing circumstances afforded by contemporary Internet techniques undermines the foundations of traditional data privacy law.

The outcome of contemporary data privacy regulatory limitations and the complex processing environment compromises the level of data privacy afforded to individuals. Individuals frequently find themselves trapped in processing conditions they do not understand and have no easy way to control. For instance, a simple change of the "privacy settings" in a social network website may affect the real, local lives of individuals all around the world. However, if they wished to object they would discover that they have to go up against a foreign

---

[124] According to Bennett and Raab, even in 2006, "four possible visions of privacy" could be identified: "the surveillance society, an incoherent and fragmented patchwork, a world of privacy haves and have-nots, and a trading-up to global privacy standards. Our analysis suggests the second scenario is the most plausible[.]" BENNETT & RAAB, *supra* note 6, at 295; *see also* Charles Raab & Bert-Jaap Koops, Privacy Actors, Performances and the Future of Privacy Protection, *supra* note 14, at 209.

[125] According to Bennett and Raab, "the ability of any one jurisdiction to protect the privacy of its citizens through public policy is inescapably linked with the actions of public and private organisations that operate outside its borders[.]" BENNETT & RAAB, *supra* note 6, at xv; *see* also Yves Poullet, *Transborder Data Flows and Extraterritoriality: The European Position*, 2 J. INT'L COM. L. & TECH. 152 (Issue 3, 2007).

corporation possibly in a far-away country, where their national law (and local data protection agency) may have little to offer.

Effective international governance for data privacy is therefore urgently needed. The legal[126] options available to accomplish this vary considerably, but they could perhaps be categorized into the following three scenarios. *First*, the *status quo* is maintained, through continued development of the international or regional regulatory frameworks currently in effect and treatment of processing challenges as best as possible on an *ad hoc,* perhaps technology-assisted, basis. *Second*, the European General Data Protection Regulation, which by mid-2014 is expected to replace the EU Data Protection Directive, directly or indirectly, assumes the role of the international standard for data privacy protection. *Third*, an international data privacy organization is established to warrant international data privacy governance. Such an organization could get a head start by making use of current global data privacy protection initiatives, such as the Madrid Declaration, or global-reaching documents already in place, such as the UN Guidelines; after all, the field could refer to the example of other sectors that achieved international governance status after decades of persistent efforts, despite the fact that they fostered similarly pervasive legislation, such as copyright.

FIRST SCENARIO: MAINTAIN, AND FURTHER ENFORCE, THE STATUS QUO

The merits of the current international governance model for data privacy ought not be overlooked: it is a pluralistic, cosmopolitan model that caters to a multitude of alternatives derived directly from stakeholders; in practice, it is a democratic model for the regulation of data privacy, allowing countries and their elected governments to choose the option that best suits their needs and culture.[127]

---

[126] Colin Bennett & Charles Raab, *The Governence of Global Issues: Protecting Privacy in Personal* Information. European Consortium for Political Research Joins Sessions of Workshops 24 (Mar. 28-Apr. 2, 2003) (Bennett and Raab "contend that privacy is better seen as also a social value rather than just as an individual right . . . in certain contexts the government regulators are not necessarily the most important actors, and the laws they enact are not necessarily the most important instruments . . . the governance of privacy has become a complex phenomenon that involves a plurality of actors and a range of methods of operation and coordination[.]"); *see also* BENNETT & RAAB, *supra* note 6, at 294.

[127] *See* Christopher Kuner, *An International Legal Framework for Data Protection, supra* note 30; Burkard Eberlein and Abraham L. Newman, *Escaping the International Governance Dilemma? Incorporated Transgovernmental Networks in the European*

This "multi-faceted international approach" should therefore not light-heartedly be dismissed; it developed over decades of intensive data privacy norms application, represents a substantial investment in resources, and despite its inherent limitations,[128] has undoubtedly created a certain level of privacy protection that individuals around the world enjoy today.

The main challenge of this approach is its efficiency within a global, processing-intensive environment. Emerging (the "cloud," location-based services) or forthcoming (ubiquitous computing, the "Internet of things") information technology trends require an unprecedented level of international cooperation in order to adequately protect individual rights and business interests.

However, until today it could be held that international cooperation only took place when absolutely necessary and only with a strict, limited scope. For instance, the EU and the United States cooperated only in response to business or national security threats, but their solutions remain fragmented and piecemeal. In the same context, the EU concluded special bilateral agreements with countries such as Canada and Australia when national security reasons imposed the exchange of passenger data.

In response, perhaps inherent limitations on the expansion of the current regulatory data privacy system to cater to the new global processing environment, assistance could come in the form of technological solutions and flexible regulatory schemes. [129]

Technological solutions that could respond to either a market need or a regulatory requirement could involve the implementation of Privacy By Design[130] system architecture or the employment of Privacy Enhancing Technologies for the protection of personal information. Under the same category should also be listed any requirements as to

---

Union, GOVERNANCE: AN INT'L J. OF POL'Y, ADMIN., & INST. 44 (Jan. 2008). This appears, after all, to be a common international governance problem.

[128] Raab and Koops, Privacy Actors, Performances and the Future of Privacy Protection, *supra* note 14, at 220 ("Pluralism of regulatory activity is one thing, but dilusion [sic] is the other side of the coin, particularly if there is no director to guide the actors[.]").

[129] *See* Ilias Chantzos, Global *Compatible Standards* of *Privacy and Data Protection*, presentation during the International Data Protection Conference, Budapest, 9, 12, June 13, 2011; Slawomir, *Cloud Computing; Security and Privacy Issues*, presentation during the International Data Protection Conference, Budapest, 15-18 June 2011.

[130] *See* 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) Article 23 (2012).

the preset "privacy settings" in software applications, such as Internet browsers. On the other hand, flexible regulatory solutions that would address the need for an increased level of international cooperation could involve the further development of Binding Corporate Rules (BCRs), which are globally acknowledged privacy standards, and other (admittedly, self-regulatory) instruments.[131]

For the current democratic and cosmopolitan data privacy regulation model to continue to proliferate, international cooperation has to become both easier to achieve and more generous. In the past, legislators were practically dragged to negotiations when pressed for immediate action. Under such law-making circumstances, output has been, expectedly, limited in scope and ambition. Technology could, if the market or regulators so require, step in and provide useful solutions. Flexible, self-regulatory instruments could also further the data privacy international governance purposes. Even in this case, however, it remains to be seen whether this combination of solutions will ultimately create a secure, comprehensive personal data processing environment according to both individuals' and businesses' expectations.

SECOND SCENARIO: THE AMENDED EU DATA PROTECTION DIRECTIVE (THE 'EU GENERAL DATA PROTECTION REGULATION') BECOMES THE INTERNATIONAL DATA PRIVACY STANDARD

Despite the fact that within some fifteen years of intensive application, only a handful of countries have managed to pass its *adequacy* criterion,[132] which allows personal data transfers to them, the EU has been extremely active in exporting its data protection model.[133] The European data protection model presents a ready-made solution of substantial depth that can be tempting to countries with no previous data privacy experience.

---

[131] *See* Christopher Kuner, Global Standards for Data Protection and Privacy, Presentation during the International Data Protection Conference, Budapest, 39-41 June 2011.

[132] *See* Christopher Kuner, *Developing an Adequate Legal Framework for International Data Transfers*, in *Reinventing Data Protection?*, ed. Serge Gutwirth et al. (Springer Science, 2009), 262.

[133] See Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108*, 2 INT'L DATA PRIVACY LAW 68-92 (Issue 2, 2012).

The EU data protection model is temporarily under heavy restructuring.[134] A series of internal developments made a general review necessary: the ratification of the Lisbon Treaty, which acknowledged a "right to data protection"[135] separate from the "right to privacy"; the aging provisions of the (1995) Data Protection Directive;[136] the release of sector-specific instruments such as the ePrivacy Directive;[137] and the intra-EU PNR Directive, which is still under development. In addition, already-existing data protection instruments that protect security-related processing, such as the 2008 Framework Decision,[138] must be properly incorporated into the new scene.

The European Commission began work on the review of the EU data protection framework in 2009 and presented the first drafts in early 2012. Its intention is to replace the entire EU data protection edifice by means of two instruments: the EU General Data Protection Regulation,[139] intended to replace the EU Data Protection Directive 95/46/EC, and the Police and Criminal Justice Data Protection

---

[134] For a concise summary on the on the pre-EU General Data Protection regulation environment, see Peter Hustinx, *Recent Developments in the European Union*, 30 Years After: The Impact of the OECD Privacy Guidelines," Joint ICCP-WPISP Roundtable Paris (Mar. 10, 2010).

[135] Treaty on the Functioning of the European Union art. 16.1, Mar. 25, 1957, O.J. C. 83, 30.3.2010.

[136] As opened by the European Commission's Communication, A comprehensive approach on personal data protection in the European Union, COM (2010) 609 final, (Nov. 4, 2010).

[137] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended and in effect today (July 12, 2002); on its implementation see also Paul de Hert & Vagelis Papakonstantinou, *The Amended EU Law on ePrivacy and Electronic Communications after its 2011 Implementation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights*, 29 JOHN MARSHALL J. OF COMP. & INFO. LAW 29, 29-74 (2011).

[138] Council Framework Decision 2008/977/JHA of 27 November 2008 on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters.

[139] See European Commission, 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, COM(2012) 11 final.

Directive,[140] intended to replace the 2008 Framework Decision. The law-making process is expected to be concluded by 2014; the EU General Data Protection Regulation will be immediately binding upon Member States.[141]

Given the limited scope of the EU Police and Criminal Justice Data Protection Directive (it only applies to security-related processing), the EU General Data Protection Regulation is expected to become the basic data protection text in the EU. The draft Regulation is an impressive text (of some 90 articles and 100 pages) that builds on the basic Data Protection Directive assumptions (the Fair Processing Principles, the special individual rights of information, the establishment of an independent and dedicated state controlling mechanism, and access and rectification), incorporating the lessons learned over more than fifteen years of rigorous implementation, and updating the assumptions in contemporary processing circumstances. Among its novelties are the introduction of a "right to be forgotten" and a "right to data portability," the application of Privacy By Design system architecture, the introduction of a "principle of accountability" intended to levy the bureaucratic burden off data controllers, and the introduction of "data protection impact assessments."[142] The draft Regulation maintains and furthers, the *adequacy* criterion.[143] By now, the importance of international personal data transfers is acknowledged and a whole Chapter is dedicated to their regulation.[144] Practices of the past (adequacy findings, one-off appropriate safeguards' establishment, binding corporate rules, and limited, space

---

[140] See European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (Jan. 1, 2012).

[141] Meaning that no harmonization of national laws among Member States through the introduction of relevant acts within a few years deadline, as is the case with Directives, is needed. *See* Treaty on the Functioning of the European Union art. 288, Mar. 25, 1957, O.J. C. 83, 30.3.

[142] *See also* de Hert & Papakonstantinou, The Proposed Data Protection Regulation Replacing Directive *95/46/EC: A Sound System for the Protection of Individuals*, COMPUTER LAW & SECURITY REVIEW 28 142 (2012); Paul de Hert et al., *Principles and the Proposed New Data Protection Regulation*, The European Journal for Social Science Research-Innovation, Sept. 21, 2012.

[143]Treaty on the Functioning of the European Union art. 41, Mar. 25, 1957, O.J. C. 83, 30.3.

[144] Personal Data Act 523, Chapter V (1999).

for derogations) are laid down in detail and occupying whole Articles.[145] International cooperation for the transfer of personal data is requested.[146] Altogether, the basic EU principle remains unchanged: personal data may flow out of the EU only to destinations where appropriate (essentially, EU-like) data protection safeguards are in place.

The EU General Data Protection Regulation, when it comes into effect, could ultimately be elevated to an international standard.[147] In the absence of a set of regulations that are operational and directly transferable at the national level, the EU data privacy model will present undoubted efficiency advantages to any newcomer in the field.[148] In addition, given the EU's significance at the global level, it is likely that more countries, especially those with no firm resolutions as to their preferred data privacy regulatory model, will adopt its data protection model in the hope of acquiring an *adequacy* finding by the European Commission. After all, the EU could exercise indirect pressure to this end by requesting that any Internet site targeting EU citizens abide by EU data protection rules, regardless of the site's place of origin, [149] further strengthening the Regulation's "extraterritoriality" effect.[150]

---

[145]Treaty on the Functioning of the European Union art. 41, 42, 43 & 44, Mar. 25, 1957, O.J. C. 83, 30.3.

[146] Treaty on the Functioning of the European Union art. 45, Mar. 25, 1957, O.J. C. 83, 30.3. In Article 45

[147] However, there seems to be little hope for future convergence on data privacy between the EU and the USA (according, for instance, to Westin, "we deliberately chose to break with European institutions in 1776, and it would be remarkable if we thought that a return to deference without agreement was the right course in 1996", quoted in BENNETT & RAAB, *supra* note 6, at 114).

[148] *See also* Graham Greenleaf, *Do Not Dismiss 'Adequacy': European Data Privacy Standards are Entrenched*, 114 PRIVACY LAWS & BUSINESS INTERNATIONAL REPORT 16-18 (Dec. 2011).

[149] Significant work has been already undertaken to this end; see the Article 29 Data Protection Working Party Working Document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites; see WP 56 (May 30, 2002) or its Opinion 1/2008 on data protection issues related to search engines. *See also* Likke Moerel, *The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?*, 1 INT'L DATA PRIVACY LAW 28-46 (2011).

[150] *See* the Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law; and Rosa Barcelo, Global Dimension of Data Protection, presentation during the International Data Protection Conference, Budapest, 16-17 (June, 2011).

To the same end, an additional facilitator is Convention 108 of the Council of Europe, which is also being amended. Under its Protocol, the Convention has come closer to the EU data protection model, and the fact that it is open for ratification by non-Member States allows for another adoption alternative to third-party (non-European) states.[151]

However, the EU data privacy model, whether in the Data Protection Directive 95/46 or in the draft Regulation intended to replace it, is by no means a panacea. It builds upon and reflects European state organization concepts that may not be suitable to all countries around the globe.[152] For instance, it requires that a new and independent administrative authority (the "data protection authority') be installed into state bureaucracies. This administrative authority will be authorized to control practically any and all personal data processing within the country. In federations, the new authority will be needed at both state and federal levels. Given the exponential increase of such processing that by now affects all sectors of human life, in practice the new authority would be a powerful and influential new player in modern public administrations, a fact that may not sit well with states that have no previous experience with such mechanisms. In addition, the EU data privacy model imposes a set of data processing principles, the added value of which may not immediately become apparent to everyone. For instance, although it is likely that nobody would object to the "data quality" principle (that data be kept accurate and up to date), the "purpose specification principle" asks that no data is processed, or even collected, unless the purpose of the processing is known in advance, and that once such purpose is served then the data need to be deleted—admittedly, a far from self-evident data processing practice.

Additionally, the EU data privacy model imposes a set of data processing principles, whose added value may not become immediately apparent. For instance, while few would object to the "data quality" principle (that data be kept accurate and up to date), the "purpose specification principle" states that no data should be processed, or even collected, unless the purpose of the processing is known in advance; and once that purpose is served, the data must be

---

[151] With Uruguay probably being the first in a long list of applicants. *See* Jörg Polakiewicz, Convention 108 as a Global Privacy Standard? Presentation during the International Data Protection Conference, Budapest 16-17 (June, 2011); Graham Greenleaf, *The Influence of European Data Privacy Standards Outside Europe*, Int'l Data Privacy Law, Vol. 2 Issue 1 (2012).

[152] *See also* Privacy Laws: Private Data, Public Rules, THE ECONOMIST (Jan. 28, 2012).

deleted—admittedly, a far from obvious data processing practice. The same is likely true of the EU data protection model's set of specific rights afforded to individuals. Although the right of individuals to ask for their data to be rectified if incorrect appears unquestionable, their right to be informed that information is being collected on them with the intention of later being processed, and their right to access a complete copy of their file together with technical details of such processing, may be at times hard to explain.

In essence, the EU data protection approach refers to a rigid and structured data protection model that may appeal to organized (mostly Western-style) bureaucracies, but may deter newcomers in the field, particularly emerging economies that may see some benefit in adopting a more flexible and relaxed solution.

THIRD SCENARIO: ESTABLISHMENT OF AN INTERNATIONAL DATA PRIVACY ORGANIZATION (FIVE ARGUMENTS)

The general acknowledgement of the need to better cooperate at an international level when regulating data privacy has led to public discussions concerning the possibility of a single international data privacy framework. This option is widely discussed in international data privacy *fora* and legal theory. However, while its merits are undeniable, its plausibility is frequently and justifiably challenged.

The introduction of a single international data privacy framework has been requested by a broad, diverse circle of stakeholders, ranging from the Data Protection and Privacy Commissioners[153] to Google.[154] However, global consensus ends at the intention. Agreement over the regulatory means to accomplish this has failed, let alone an agreement on what substantive provisions such an instrument would include.

A number of complex factors seem to make international governance through an international legal framework impossible. Among them, these are perhaps the greatest obstacles:

---

[153] *See* The Montreux Declaration of 2005; the Madrid Resolution of 2009, *supra*.

[154] *See* de Terwangne, Is a Global Data Protection Regulatory Model Possible, 175.

FIRST, THERE IS NO COMMON GLOBAL PERCEPTION OF PRIVACY AND DATA PROTECTION[155]

Data protection and privacy (even in its data privacy format) may have been used interchangeably for the purposes of this paper, but this is an oversimplification. The right to privacy is different from the right to data protection and data privacy or information privacy should probably be used as synonyms to data protection, instead of merely "privacy." The right to privacy is related to the right to data protection, but it is not "an identical twin."[156] In practice, there may be occasions where the right to data protection is applicable on a given set of data, but processing of these data at the same time does not infringe the given individuals' right to privacy.[157]

Unfortunately, the above distinction is one that is only recognized by the EU. In other parts of the world, this distinction remains unrecognized, and in some cases, a right to data privacy has not even been developed. The resulting situation creates insurmountable difficulties for the creation of an international framework for data privacy, Unless they aim at developing general principles and focus on specific topics, avoiding the details of implementation, any relevant initiatives would fail to even agree upon an agenda.

SECOND, THERE IS A LACK OF INSTITUTIONAL INTERNATIONAL COOPERATION

After close observation of the data privacy output created by international organizations, it becomes apparent that work is mostly undertaken in parallel. Despite the common challenges regarding processing methods, efforts and resources that are both aimed at

---

[155] *See id.* at 180.

[156] See Paul de Hert and Serge Gutwirth, Data Protection in the Case Law of Strasbourg and Luxembrourg: Constitualisation in Action, in Reinventing data protection?, ed. S Gutwirth et al. (Dordrecht: Springer Science, 2009), 3-44.

[157] This becomes clear in European Court of Human Rights case law: the ECHR distinguishes between 'personal data that merit protection' and 'data that do not'; to-date, processing of personal data is excluded from the privacy scope when (1) the data as such are not considered as private, (2) when there are no systematically stored images or sound recordings, or other data, (3) when the data are not systematically stored with the focus on the data subject, and (4) when the data subject could reasonably expect the processing. *See id.*; *Olivier de Schutter,* Vie Privée Et Protection De L'individu Vis-À-Vis Des Traitements De Données À Caractère Personnel, R.T.D.H.: 148 et seq. (May 4, 2000).

research and law-making, are apparently duplicated. Issues like profiling, RFID, the "Internet of things," national security processing and cooperation, social network websites, and Internet search engines have attracted significant attention from many international organizations in the data privacy field (the OECD, the Council of Europe, the UN, and the EU). However, none of these organizations (apart from the Council of Europe and the EU) seems to be undertaking positive action[158] towards modeling its own data privacy according to that of any of the others.[159]

The more scholarship develops on the above international models (through position papers, task forces, research and the resulting norms) without international cooperation, the more divergent they will become, making it more difficult to achieve future consensus on a single regulatory model. After around thirty years of intensive work and parallel development of varying data privacy models, the international data privacy scene appears confusing. In theory, a country could have ratified the Council of Europe Convention 108 and be a member of the OECD, but still have not provided an *adequate* level of protection by the European Commission. Another country that is a member of the APEC may ratify the Council of Europe Convention 108 but not be a member of the OECD, and not have passed the EU *adequacy* criterion. Voluntary[160] international[161] regulations help the field of data privacy only if they do not adopt different legal models parallel to each other.

---

[158] Admittedly, the Council of Europe Convention and the OECD Guidelines both note that while elaborating their respective provisions the other instruments workings were taken into consideration. *See* the Explanatory Memorandum of the Guidelines and the Explanatory Report of Convention 108, *supra*, par. 90.

[159] Neither is any international organization or observatory (apart from NGOs such as Privacy International) cataloguing data privacy developments in all countries around the world (therefore, Kuner, for instance, can only estimate that "[i]f one includes all such instruments, then the number of countries regulating transborder data flows in some form, or that have the possibility of doing so, is close to 100" in Christopher Kuner, Regulation of Transborder Data Flows Under Data Protection and Privacy Law, 20.). This is a well identified shortcoming; see Michael Kirby, Privacy Protection, a New Beginning: OECD Principles 20 Years on, (presented at the 21st International Conference of Privacy and Data Protection Commissioners, Hong Kong, 1999), http://www.austlii.edu.au/au/journals/PLPR/1999/41.html.

[160] Even the EU may be perceived as "voluntary" for nonmember States, if they decide to submit themselves to qualifying for the "adequacy" criterion.

[161] Even the Council of Europe Convention may be perceived as "international" by now, because it is open for signature to nonmembers.

THIRD, THERE ARE DIFFICULTIES IN IDENTIFYING THE PROPER LEGAL INSTRUMENT FOR INTERNATIONAL GOVERNANCE

International governance has itself been affected by contemporary complexity. The regulatory options available today far exceed those available a few decades earlier. In addition, the number of global players has increased substantially. From the handful of international organizations of the early 1980s, a multitude of institutional and, crucially, non-institutional participants (NGOs, international bodies, user groups, etc.) have been added. In short, if international data privacy governance in the form of a single international legal framework was attempted now, there would be more means by which to achieve the framework and a greater number of parties that would participate in the framework's formulation than there were when the first relevant instruments were released.

Therefore, even if an agreement was reached on the exact content of data privacy, substantial difficulties would lay behind each of the regulatory options available for the creation of a single international legal data privacy framework.

Options for regulatory vehicles that could accommodate such a framework include, among others: the introduction of a new multilateral treaty or convention, the introduction of a model law that states can enact into their national laws; the elaboration of standard terms and conditions that can be incorporated into contracts and other documents between private parties; or even a codification of custom and usage promulgated by a nongovernmental organization.[162]

However, each one of the above solutions has to address seemingly insurmountable difficulties.[163] A multilateral convention would likely take many years to conclude and still could not achieve the desired harmonizing effect. [164] Apart from failing to achieve obvious international harmonization, adopting regional conventions and treaties already in effect would have to resolve certain inherent restrictions that each one of the available options presents. A model law to be incorporated as in national jurisdictions could be difficult to

---

[162] *See* Christopher Kuner, An International Legal Framework for Data Protection, 311.

[163] In fact, so many that Kuner remarks that "the time does not yet seem ripe for a binding international legal instrument on data protection" (p.316); see also Bygrave, referenced in the same paper (p.315).

[164] A claim also confirmed by the time needed (almost a decade) for the UN to release its Guidelines.

develop and would probably not achieve a harmonizing effect. Technical data privacy standards to be incorporated into data processing systems could not replace international regulation. Lastly, international voluntary instruments (codes of practice, recommendations, etc.) are of limited use for the purposes of data privacy regulation.

On the other hand, a number of enabling factors press towards the opposite direction, that of international cooperation:

FIRST, THERE ARE COMMON PROBLEMS, WHICH ARE COMMONLY FELT.

As noted, today the international data privacy agenda is set by two external factors: information technology [165] and political developments.[166] In a globalized world such problems are common and challenges are commonly felt reword. Electronic commerce models are global in the sense that if they are not globally singular (for instance, Facebook, Google, etc.), they are reproduced in similar terms locally (local social networking websites or search engines). In addition, the political agenda is equally global. For instance, after 9/11 security-related personal data processing exponentially increased its global importance. Attempting to resolve global phenomena through local or *ad hoc* international solutions presents obvious efficiency limitations.

SECOND, PRESSURE FROM THE PUBLIC

Setting any plausibility concerns aside, virtually everyone involved in the data privacy process sees the impracticality of the current regulatory model, from a human rights standpoint and from an international business point of view, and presses for the adoption of a single international legal framework.[167] Everybody would prefer their

---

[165] To be taken into consideration not only as of a technical but also of a social nature, in order to cover essentially social phenomena such as Facebook, YouTube, etc.

[166] *See* Paul de Hert and Vagelis Papakonstantinou, *The Data Protection Framework Decision of 27 November 2008 Regarding Police and Judicial Cooperation in Criminal Matters-A Modest Achievement However Not the Improvement Some Have Hoped for*, 25 *COMPUTER L. & SECURITY REVIEW* 403ff (2009).

[167] In this context, Burkert notes that "it can at least reasonably be assumed that those suggestions for restructuring data protection will have the best chance of being adopted, which are the most responsive to social change and the concerns this change evokes"; see

country's own data privacy model to be upgraded into international status. While this is understandably not possible, the momentum is favorable and broad consensus is attainable in light of international data privacy challenges.

THIRD, THERE IS A SHORTAGE OF RESOURCES AND A NEED TO GLOBALIZE INFORMATION TECHNOLOGY

In the current environment of scarce financial resources, the multiplication of efforts at international level in order to address the same data privacy challenges, and the devising of complex, resource-hungry, *ad hoc* regulatory solutions is impractical. Considering this, it appears that because the need for international regulation is commonly felt and broadly shared, the introduction of a single, comprehensive international data privacy regulatory instrument regulating, in detail, each personal data processing instance in every country around the globe would most likely not be the most effective solution to address the pressing reality.

In this context, it is suggested that a new international data privacy organization be established, whose sole task would be to promote data privacy issues globally, in the same way as, for instance, the World Intellectual Property Organization (WIPO) advances the purposes of intellectual property protection. WIPO is a specialized UN agency that was established in 1967.[168] Its mission is to "to promote innovation and creativity for the economic, social and cultural development of all countries, through a balanced and effective international intellectual property system."[169] In order to achieve this, WIPO administers more than twenty international treaties and accepts member states (185 in total). WIPO succeeded the United International Bureaux for the Protection of Intellectual Property, which was established in 1893 by the Berne Convention.[170]

A number of parallels can be identified between the two systems. The importance of the copyright system, as is the case with data protection, was generally acknowledged in the late 19th century, but

---

Herbert Burkert, *Towards a New Generation of Data Protection Legislation*, in *Reinventing Data Protection?*, ed. Serge Gutwirth et al. (Springer Science, 2009), 335.

[168] By the Convention Establishing the World Intellectual Property Organization that was entered in 1967 in Stockholm and came into effect in 1970.

[169] *See* the WIPO website (www.wipo.int).

[170] Berne Convention for the Protection of Literary and Artistic Works (1886).

the protection awarded was fragmented and largely diverging among those (relatively few) states that experimented with the new field of law. The Berne Convention had to carefully balance among the legal systems already in place, without however this meaning that the resulting text made everybody happy (or, for the same purposes, an immediate signatory to the Convention). The Bureaux was established in order to administer the Convention; however, after several decades of intensive application, intellectual property, within the WIPO meaning, is practically part of the international law acquis.

These lessons are applicable to data protection. A new international data privacy organization created to administer an international data privacy instrument that would attempt to harmonize critical points of divergence would probably be the only plausible means by which to achieve global data privacy protection in the foreseeable future.

Luckily, the establishment of such a new international organization does not necessarily mean that a new international data privacy instrument, even within the relaxed lines described above, also needs to be introduced, at least at this stage. Instead, an instrument already in effect could be utilized: the UN Guidelines. They would constitute an obvious choice to this end–the mere addition of a new office to administer the Guidelines' application would suffice.

Despite the fact that the UN Guidelines have attracted very limited attention and are apparently abandoned (not updated or further developed or amended in any way) by the organization that released them, they present a series of incontestable advantages. They have been in effect since 1990, so valuable time need not be wasted in releasing a new set of rules and achieving the respective consensus. They avoid unique national or regional approaches (for instance, the rigid EU data protection model that seems to deter a number of countries around the globe). They have the broadest circle of recipients possible, are equally concerned with the human rights and transborder data transfers perspective, and they already include an adequate set of data privacy rules. Additionally, their UN origin makes the establishment of a new UN agency, just as the case is with WIPO, perhaps easier (or, at least, less time consuming), and also assuages concerns (for instance, from developing countries or countries not located in Europe or North America) that the current European,

APEC, or even OECD models are unsuitable outside their geographical boundaries.[171]

Once established, this organization would subsequently strive to achieve global harmonization and develop a single international data privacy framework. Exactly the same way the Berne Convention has been repeatedly amended to reflect technology and other developments, the original data privacy UN Guidelines could be expanded or added to in order to accommodate new processing circumstances. An obvious aim would also be the convergence of the various data protection models already in place around the globe—most notably, the EU model with that of non-EU countries (particularly with the US), with the additional benefit, however, that negotiations will not be bilateral and the input of third countries will also be heard. The international instruments already in effect (the OECD Guidelines or Convention 108, even after they have been amended respectively) could contribute to this goal, because their provisions are not substantially different from those of the UN Guidelines. Obviously, this by no means is an easy task, but one should note that progress in the intellectual property field was also particularly slow.

The future of humanity is now intrinsically connected to information technology and the Internet. Data privacy problems are listed among the top issues standing in the way of global acceptance of the new medium and are only expected to become more important in the future. Unless the public is reassured that individuals' private lives are rigorously protected in modern ubiquitous processing environments, the public will remain suspicious as to the intentions of new data controllers or the benefit of incorporating their applications into its life, developing thus an adversarial, unwelcome effect (Or perhaps fall into a surveillance trivialization ("banalisation de la surveillance") (an equally disturbing alternative.).[172]

---

[171] Although the same advantages are more or less held met in the OECD Guidelines or, even, in the Madrid Declaration, these instruments lack the UN element of the Guidelines.

[172] *See* Rocco Bellanova, Paul de Hert & Serge Gutwirth, Variations sur le thème de la banalisation de la surveillance (Some thoughts on the issue of surveillance trivialisation). « Mouvements » (Movements), issue Sous contrôle (Under Control). Gouverner par les fichiers, n. 62, pp.46 - 54, eds. Meryem Marzouki et Patrick Simon, published by La Découverte, (2010).

FINAL REMARK: REDISCOVERING THE ROLE OF THE UN IN DATA PRIVACY

The 30th anniversary of both the Council of Europe Convention 108 and the OECD Guidelines marks a unique historical opportunity for the international data privacy field. In practice, three out of four basic international data privacy instruments, the OECD Guidelines, the Council of Europe Convention 108, and the EU Data Protection Directive, are currently in the process of being amended or reevaluated in order to address the current processing complexities. This coincidence could ultimately prove to be a blessing or a curse for the data privacy field: if each instrument takes positive steps to converge with the others, creating in essence a single international regulatory framework, international governance of data privacy would benefit from an unexpected gift. However, if on the contrary, each model decided to further its own purposes and follow its own path, one more obstacle to the creation of a single regulatory framework would be erected by the release of yet another generation of diverging approaches.

Because the merits of uniform international governance of data privacy within a globalized, interconnected processing environment are generally not challenged, attention should be given to the plausibility of such an outcome. In this context, the establishment of a new international organization with a concrete data privacy mandate could address contemporary concerns and also constitute a permanent mechanism for international data privacy cooperation for the future. The 1990 UN Guidelines, although under-used and more or less abandoned, even by the organization that released them, offer an adequate data privacy regulatory framework that is at the same time flexible enough to constitute the first global standard. Once established, this organization should then try to create a detailed, comprehensive international regulatory framework for the future.

Data privacy challenges may appear urgent from time to time, but their number is not finite. Even if those of concern today are successfully addressed, new ones will soon enough emerge. One should not forget that most of the major sources of concern today (search engines, 9/11 and its aftermath, social networking websites) have a life span of less than a decade. While efficiently resolving current issues is a cause worth fighting for, the nature of problems mean that the most difficult tasks are yet unresolved and indeed lie ahead. Therefore, although time constraints should certainly be taken into consideration, one ought not forget that a sound, comprehensive data privacy system should be constructed for the future.

In this context, the creation of a single international regulatory model for data privacy seems inevitable. Until either the amended Council of Europe Convention 108 or the EU General Data Protection Regulation—the only bodies that provide a comprehensive solution and are export-oriented—are raised to the task, the means by which to establish a new, subject-specific international organization or patient management of data processing are irrelevant. The need is for international governance of data privacy to move from its contemporary role as a horizontal, agenda-setting process, to a globally harmonizing one. This is a task of critical importance in order for information technology and the Internet to fully benefit humanity. Public trust will not be vested in the new medium if is not perceived as carefully observing fundamental human rights. Global cooperation is therefore urgently required in order to resolve a problem that, if left alone, threatens nothing less than "the future of the human condition."[173]

[173] Michael Kirby, Privacy Protection, a New Beginning: OECD Principles 20 Years on, Presented at the 21st International Conference of Privacy and Data Protection Commissioners, Hong Kong (1999).