WALLED GARDENS OF PRIVACY OR "BINDING CORPORATE RULES?": A CRITICAL LOOK AT INTERNATIONAL PROTECTION OF ONLINE PRIVACY

Joanna Kulesza[*]

I. INTRODUCTION

Protecting Internet users' privacy is a growing concern in the era of cloud computing, especially when one considers the absence of any effective international solutions. The existing Safe Harbor Privacy Principles, which were meant to guarantee stringent European Union (EU) data protection standards for U.S. companies, are ineffective. In order to protect the privacy of Internet users, the existing trans-Atlantic personal data exchange agreements need to be amended. This article presents the latest EU-proposed development in the area—a regulatory model based on amended Binding Corporate Rules ("BCR" or "BCRs")—as introduced by EU Justice Commissioner Reding in late 2011. The 2012 reform of EU data protection regulations includes proposals to modify the EU approach to corporate personal data protection policies and to simplify regulations for companies participating in the EU market. The planned changes in EU legislation would have worldwide effects on international companies' online activities in transboundary cyberspace.

After describing the BCR proposal, this article will consider the likelihood of both its application as well as alternative scenarios to the EU-proposed model. The most likely alternative depicts a gloomy vision of loosely intertwined, firewall-guarded national areas in cyberspace where privacy would be secured according to varying national standards—a "splinternet" operating on elaborate software and stringent legislation. Such national "walled gardens" of privacy would well resemble the current trends in national cybersecurity policies, where an increasing number of states are opting to limit their residents' access to the global network with elaborate software and legislation. This pessimistic scenario would mean the end of the global information society, whose bastion of liberty is the boundless cyberspace. This article offers an international-law solution to this challenge and emphasizes the significance of the BCR's proposal.

* Assistant Professor, Department of International Law and International Relations, Faculty of Law and Administration, University of Lodz, Poland.

II. BACKGROUND

Defining privacy has always been a challenge, not only when it comes to identifying its scope, but also when one attempts to portray its origins. In U.S. jurisprudence, Samuel Warren and Louis Brandeis are hailed by most scholars as authors of the "right to be let alone" concept, which introduced the notion of privacy in the late nineteenth century.[1] Around the same time in Germany, Josef Kohler discussed a similar concept.[2] However, French courts are credited with recognizing the right to private life as early as the mid-nineteenth century.[3]

Initially taken with much skepticism,[4] the idea of legal protection for one's private life developed and found its undisputed place in international jurisprudence.[5] Although the right to privacy is no longer questioned, a definition of privacy, vital for ascertaining the scope of appropriate legal protection, is still hard to find. The reasons for this predicament are twofold.

The first challenge is the disaccord on the actual nature of the term. Privacy is directly related to human rights and personal data protection in Europe, while in the United States and numerous other jurisdictions, it is perceived as an element of commercial enterprise.[6] Even when these two different understandings of privacy meet in the Organization for Economic Co-operation and Development (OECD) forum, and it is assumed that personal data is a component of the individual's right to privacy, the ways and means in which to protect that right strongly differ. Unavoidably, this disac-

---

1. *See, e.g.*, Harry Kalven, Jr., *Privacy in Tort Law—Were Warren and Brandeis Wrong*?, 31 LAW & CONTEMP. PROBS. 326, 327 (1966); Robert C. Post, *Rereading Warren and Brandeis*: *Privacy, Property, and Appropriation*, 41 CASE W. RES. L. REV. 647 (1991). *But see* David W. Leebron, *The Right to Privacy's Place in the Intellectual History of Tort Law*, 41 CASE W. RES. L. REV. 769, 775–77 (1991) (accrediting E. L. Godkin with formulating the need of protection of privacy in E. L. Godkin, *Libel and Its Legal Remedy*, 12 J. SOC. SCI. 69 (1880)).

2. Josef Kohler, *Ehre und Beleidigung*, 47 GOLTDAMMERS ARCHIV FÜR DT. STRAFRECHT 1–48 (1900); *see* Ulrich Falk & Heinz Mohnhaupt, *Das Bürgerliche Gesetzbuch und seine Richter: zur Reaktion der Rechtsprechung auf die Kodifikation des deutschen Privatrechts (1896-1914)*, 359–60 (2000).

3. ANDRE BERTRAND, DROIT A LA VIE PRIVÉE ET DROIT A L'IMAGE 2 (1999). For a comprehensive study on the genesis of privacy see ARWIND MEDNIS, PRAWO DO PRYWATNŚCI A INTERES PUBLICZNY 58 (2006).

4. *See* Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

5. *See* Erwin N. Griswold, *The Right to be Let Alone*, 55 NW. U. L. REV. 216, 218–20 (1961).

6. *See* COLIN J. BENNETT, REGULATING PRIVACTY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 45–94 (1992); David L. Baumer, Julia B. Earp & J.C. Poindexter, *Internet Privacy Law: A Comparison Between the United States and the European Union*, 5 COMPUTERS & SEC. 400, 400–12 (2004) (comparing the EU data protection regime and the California Online Privacy Protection Act of 2003).

cord renders ineffective any legal tools introduced to protect this perceived privacy globally.

The second challenge stems from the shifting scope of privacy. In European jurisprudence, the term has been comprehensively defined through the application of the Convention for the Protection of Human Rights and Fundamental Freedoms ("The European Convention on Human Rights" or "ECHR") and might seem consistently understood throughout all forty-seven ECHR state parties. The challenges brought about by the era of cyberspace make this pillar of human rights tremble. New challenges to the seemingly well-defined scope of the term are brought about by services such as Google Street View and new categories of personal information like geolocalization data enabled through mobile devices.[7] It is unclear whether the right to have one's home portrayed and identified online to all users worldwide or to have information of one's real-time location enabled to mobile phone operators, Internet service providers, or Internet users should be recognized as elements of the right to have one's privacy protected and, therefore, secured with additional legal safeguards. Adding to these questions are the difficult issues of online jurisdiction over Internet service providers (ISPs) or Internet content providers (ICPs). Whether national courts and authorities, such as data protection ombudsmen, have jurisdiction over, for instance, Facebook's geolocalization data of its users within its *Places* service or over Google photographing local streets for its Google Street View is defined differently by national courts.[8] Durability, accessibility, and other unique characteristics of electronic data induce new proposals for complementing the right to privacy with, for example, a right to be forgotten[9] or automated data deletion after a certain, arbitrarily set period of time.[10]

When attempting to define privacy, legal scholars and practitioners alike traditionally resort to one of three sets of norms. The most frequently

---

7. *See* EUR. PARL. ASS., *The Protection of Privacy and Personal Data on the Internet and Online Media*, 36th Sess., Res. No. 1843 (2011), *available at* http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta11/ERES1843.htm.

8. German courts have jurisdiction over Google Street View filming Berlin streets. *See* Cyrus Farivar, *Berlin Court Rules Google Street View is Legal in Germany*, DEUTSCHE WELLE (Mar. 21, 2011), http://www.dw-world.de/dw/article/0,,14929074,00.html. While the Polish Personal Data Ombudsman is equally certain, Polish courts have no jurisdiction over Facebook, even though it offers its services in Poland. *See Facebook poza Polską Jurysdykcją: Nie Można go ani Pozwać, ani Skontrolować* [*Facebook Outside Polish Jurisdiction: Cannot be Sued or Controlled*], GAZETA PRAWNA (Nov. 19, 2010), http://prawo.gazetaprawna.pl/artykuly/466155,facebook_poza_polska_jurysdykcja_nie_mozna_go_ani_pozwac_ani_skontrolowac.html.

9. *EU Proposes 'Right to be Forgotten' by Internet Firms*, BBC NEWS (Jan. 23, 2012), http://www.bbc.co.uk/news/technology-16677370.

10. *See generally* VIKTOR MAYTER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 169–98 (2011).

used set of norms for resolving privacy issues are regulations on personal data protection. In the event these are insufficient, civil law offers protection of personal rights, which includes privacy. Should those two categories of legal safeguards not suffice, the constitutional right to privacy, understood in categories of human rights, may be evoked.[11]

A. Privacy as a Human Right

Privacy as a human right is firmly rooted in the ECHR and is recognized in the constitutions and other legal acts of member states.[12] ECHR jurisprudence recognizes the right to privacy in its Article 8 as a derivative of the right to have one's private and family life respected.[13] As such, the human right to privacy may be restricted only in certain cases detailed by the ECHR.[14] The 1953 ECHR (drafted in 1950) was one of the sources used for creating the 1966 International Covenant on Civil and Political Rights of the United Nations (ICCPR), which in its Article 17 expressly protects privacy.[15] The stipulation of Article 17 resulted in similar provisions adopted in numerous constitutions and other national privacy regulations. The adoption of these provisions may be regarded as the verbalization of a bottom-line consensus on the existence and characteristics of the universal right to privacy that is understood as a human right.

When seeking the most suitable legal tool for personal privacy protection, one should analyze the international regulation of personal data protection. Various soft-law documents from multiple international forums, most significantly the OECD, reveal the universal accord of those international regulations. The non-binding yet influential 1980 OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data ("Guidelines") are an early example of a global consensus on the protection of personal

11. *See, e.g.*, Flemming Moos & Jens Kirchner, *Data Protection and Monitoring, in* KEY ASPECTS OF GERMAN EMPLOYMENT AND LABOUR LAW 109 (Jens Kirchner et al eds., 2009) (finding a "personal right" to data privacy as an employee). *See also* Kay Deaux & Brenda Major, *A Social-Psychological Model of Gender*, *in* THEORETICAL PERSPECTIVES ON SEXUAL DIFFERENCE 89 (Deborah L. Rhode ed., 1990).

12. *See, e.g.*, ALBERT J. MARCELLA & CAROL STUCKI, PRIVACY HANDBOOK: GUIDELINES, EXPOSURES, POLICY IMPLEMENTATION, AND INTERNATIONAL ISSUES 118 (2003) (referring to such a legal construction introduced in Slovenia).

13. *See* URSULA KILKELLY, THE RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE: A GUIDE TO THE IMPLEMENTAITON OF ARTICLE 8 OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS 10–19, 34–65 (2d ed. 2003).

14. *Id.* at 23–33 (discussing the application of Article 8 para. 2 of the ECHR, devoted to instances when privacy rights may be restricted).

15. International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171 ("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 . . . . Everyone has the right to the protection of the law against such interference or attacks.").

data. The Guidelines express a basic compromise on privacy as a human right.[16] That right is protected through scrupulous administration of personal data exercised by the administrator, prohibiting personal data retention (including the retention of false personal data), data abuse, and unauthorized disclosure. Interestingly, the Guidelines served as early foundations for numerous national regulations on privacy in places such as Australia, Canada, and Hong Kong.[17] In 1998, the OECD Ministerial Declaration on the Protection of Privacy on Global Networks supplemented the Guidelines' stipulations.[18]

B. Privacy and Personal Data

Presently, the most rigorous regulations on personal data protection implemented in Europe are introduced as either acts of EU law or ECHR enforcement.[19] In attempting to identify principles reflected in both EU law and ECHR decisions, one should begin by examining the 1981 Council of Europe (CoE) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[20] The Convention was aimed at strengthening "the legal protection of individuals with regard to automatic processing of personal information relating to him."[21] It obligates states to guarantee that data operators maintain the quality of information in their possession, refrain from storing operationally unnecessary information, and guard personal data against unauthorized disclosure or misuse.[22]

The EU envisaged similar principles in 1995 when it introduced Directive 95/46/EC ("Directive") on the protection of individuals with regard to the processing of personal data and the free movement of such data.[23] The

16. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, ORGANISATION FOR ECON. COOPERATION & DEV. (Sept. 23, 1980), http://www.oecd.org/document/18/0,2340,en_2649_34255_ 1815186 _1_1_1_1,00.html (last visited June 1, 2012).

17. *See* CATHERINE L. MANN, TRANSATLANTIC ISSUES IN ELECTRONIC COMMERCE 18 (2000).

18. OECD Party on Information Security and Privacy, *Ministerial Declaration on the Protection of Privacy on Global Networks* (Oct. 7–9, 1998), http://www.oecd.org /dataoecd/39/13/1840065.pdf.

19. *See* CHRISTOPHER KUNER, EUROPEAN DATA PRIVACY LAW AND ONLINE BUSINESS 1–49 (2003).

20. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, Europ. T.S. No. 108, *available at* http://conventions.coe.int/ Treaty/en /Treaties/html/108.htm (last visited May 28, 2012) [hereinafter Convention].

21. *Id.*, at Preamble.

22. *Id.*

23. 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, *available at* http://eur-

Directive is considered the groundwork for the EU's personal data protection. The Directive defines personal data by setting the limits of the legally-protected, individual right to privacy using personal data protection terms. According to Article 2 of the Directive, "personal data" is any information "relating to an identified or identifiable natural person."[24] An "identifiable person" is defined by Article 2 as "a person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his [or her] physical, physiological, mental, economic, cultural[,] or social identity."[25] The mechanism for privacy protection is based upon the Directive's data processing guidelines. Data-processing guidelines encompass various activities and regulate those conducting the processing.[26] According to Article 6, member states must ensure that data processors process personal data fairly and lawfully and only collect such data for specified, explicit, and legitimate purposes. If personal data is processed, it should be done adequately, relevantly, and not excessively in relation to the purposes for which it was collected. Processed personal data ought to be accurate and kept up to date otherwise it should be erased or rectified. The basic principle of personal data administration obligates data processors to keep personal data in a form that permits identification of data subjects but only for as long as it is necessary.[27] Because those

---

lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF [hereinafter Directive 95/46/EC] (amended by Regulation (EC) No. 1882/2003 of the European Parliament and of the Council of 29 September 2003, 2003 O.J. (L 284) 1, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:284:0001:0053:en:PDF.

24. *Id.*

25. *Id.*

26. According to Article 2, "processing of personal data . . . mean[s] any operation . . . performed upon personal data, . . . such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." *Id.* (internal quotation marks omitted).

27. The scope of privacy protection guaranteed under the provisions of Directive 95/46/EC may be substantially altered by the controversial "data retention" Directive 2006/24/EC. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 54, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:en:HTML. A practical result of introducing the regulation is that European ISPs are required to retain "traffic data" (data generated automatically during the performance of network services) about their users (data retention). The official purpose of the regulation is to facilitate the work of enforcement authorities and prevent crimes specified in the laws of each member state. The Directive was met with vigorous objection from European human rights organizations as well as negative opinions of national constitutional tribunals, finding it a gross violation of the constitutional right to privacy. *See* Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Mar. 2, 2010, ENTSCHEIDUNGEN DES BUNDESVERFASSUNGSGERICHTS

principles are enshrined within the Directive, member states should take proper measures to enforce the goal set within the Directive through appropriate, domestic legal tools.

The Directive introduces a particularly high standard of care for categories of personal data that are crucial to protecting individual privacy. Processing special data, such as information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, or sex life is generally prohibited but can take place upon individual consent given by the data subject.[28]

Subsequently, EU states adopted fitting national legislation following the Directive's definitions and procedures. In fact, many non-EU states also adopted similar models.[29] In order to face contemporary challenges to personal data protection, the EU Community instituted the Working Party on the Protection of Individuals with regard to the Processing of Personal Data under Article 29 of the Directive (WG29) with the purpose of addressing the issues vital to personal data protection as defined within the Directive.[30]

While the scope and definition of personal data protection may be well defined in Europe, the definition of privacy is not nearly as clear. Neither EU law, nor ECHR jurisprudence attempts to recognize privacy as a set of individual prerogatives. The EU recognizes the right to privacy in Articles 7 and 8 of its Charter of Fundamental Rights,[31] but European jurisprudence still treats privacy questions as an extremely fact intensive process, often producing what appears to be conflicting results. The minimum standard set by the courts could be defined as "a right to establish and develop relationship with other human beings."[32] When states aim to limit the privacy of individuals, guaranteed by Article 8 of the ECHR, they may introduce restrictions through legislation and only when it is necessary in a democratic

---

[BVERFGE] 08, 256, 263, 586 (holding the obligation imposed by the Directive 2006/24/EC unconstitutional in the light of Article 10 of the German Constitution (Grundgesetz) (Ger.)). An earlier similar decision was issued by the Romanian Constitutional Court: Curţii Constituţionale [Constitutional Court] Oct. 8, 2009, MONITORUL OFICIAL Nov. 23, 2009 (Rom.), *available at* http://www.ccr.ro/decisions/pdf/ro/ 2009/D1258_09.pdf, *translated at* http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html.

28. Article 8 paragraph 2 lists other exceptions from the prohibition on processing sensitive data and includes processing necessary data in employment law, the protection of vital interests of the data subject, or processing data that is manifestly made public by the data subject. Directive 95/46/EC, *supra* note 23, at 40–41.

29. *See* Michael D. Birnhack, *The EU Data Protection Directive: An Engine of a Global Regime*, 24 COMPUTER L. & SEC. REP. 508, 512–13 (2008).

30. Directive 95/46/EC, *supra* note 23, at 48 (working party website available at http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm).

31. Charter of Fundamental Rights of the European Union, O.J. (C 364/1).

32. *See* SELECT COMMITTEE ON THE CONSTITUTION, SURVEILLANCE: CITIZENS AND THE STATE, 2008-9, H. L.18-1, ¶123 (U.K.).

society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[33] In case of controversies, the European Court of Human Rights assesses whether such individual restriction was "necessary in a democratic society" and proportional. Ultimately, no general definition or standard for privacy exists.[34]

C. Privacy as a Personal Right

Privacy protection, as designed by data protection regulations and international human rights treaties, applies only to situations where individual privacy is threatened by government action or omission.[35] If private actors threaten privacy protection, the civil law protection of personal rights is often invoked to settle the dispute.[36] German-language countries originated civil law doctrine, which, when referring to privacy protection, refers to the theory of spheres.[37] Both German and Swiss civil law theory and practice recognize public, private, and intimate spheres, and each sphere is afforded a different degree of protection.[38] Any activity of an individual and any information about them can qualify as falling within either his or her public (Sozial- / Öffentlichkeitssphäre), private (Privatsphäre), or intimate (Intimsphäre) sphere and is awarded protection accordingly.[39] Activities that fall within the intimate sphere are given the strongest protection, while activities in the public sphere receive virtually no protection.[40]

When attempting to describe each of the three categories, one could characterize activities within the public sphere as those performed by an

33. Directive 95/46/EC, *supra* note 23, at 42.

34. KILKELLY, *supra* note 13, at 10–19, 34–65.

35. Directive 95/46/EC, *supra* note 23, at 39 ("This Directive shall not apply to the processing of personal data . . . by a natural person in the course of a purely personal or household activity."). The scope of "personal activity" in the online environment is particularly difficult to assess. *See, e.g.*, Michael D. Birnhack & Niva Elkin-Koren, *Does Law Matter Online? Empirical Evidence on Privacy Law Compliance*, 17 MICH. TELECOMM. & TECH. L. REV. 337, 380–82 (2011).

36. Although following the interpretation of Article 8, the Court imposes a positive obligation on state parties to introduce appropriate tools within national legal systems for effective protection of privacy from threats originating from actions or omissions of private individuals. *See, e.g.*, K.U. v. Fin., 2008 Eur. Ct. H.R. 1, para. 42-43, at 12.

37. *See, e.g.*, JOHANNES M. HOLZ, GOOGLE STREET VIEW – WIE DETAILLIERT DARF EIN STADTPLAN SEIN? 12–14; HELMUT KOZIOL, PERSÖNLICHKEITSSCHUTZ GEGENÜBER MASSENMEDIEN 548 (2005); HEIKE SCHAFFRIN, ALLGEMEINES PERSÖNLICHKEITSRECHT: HAFTUNG FÜR DIE VERLETZUNG DES PERSÖNLICHKEITSRECHTS DURCH KUNST 3–6 (2010).

38. SCHAFFRIN, *supra* note 37, at 3–6.

39. *Id.*

40. *Id.*

individual following their public duties and obligations, such as exercising a public function or a profession. Such activities would not fall within the ambit of privacy protection. All activities or information outside this scope are shielded by privacy protection because the activities could not be identified as falling within the public sphere. A decision to give up such protection and release private information is left to the individual, although some information within this group is given stronger protection. Any activity from the intimate sphere or information thereabout is given strenuous protection and in some cases is not revealed or used even if the person consents. This highest degree of protection is awarded to information on, for instance, sexual identity or religious beliefs. Civil law offers no definition of "intimacy"; however, the contents of the intimate sphere may be well defined by a reference to the set of "sensitive data" given particular protection under the Directive 95/46/EC.[41] The civil law protection given to all personal rights allows individuals whose privacy is threatened to demand that the potential infringement be seized (for example, infringing information is deleted or a press release is stopped), while those who already suffered infringement and harm may demand pecuniary compensation or damages.[42] Although the concept seems appealing in theory, its practical application is always challenging because there is no consensus about the scope of activities within each sphere.

D. Privacy Challenges

This brief definition of the continental concept of privacy and its protections seems to fit well with the original idea articulated by Samuel Warren and Louis Brandeis, which guaranteed individuals their "right to be let alone."[43] Twentieth century European definitions of privacy presented for research or policy purposes seem to have a similar tone. For example, upon presenting its 1900 report on Privacy and Related Matters to the House of Lords, the British Parliamentary Calcutt Committee members defined privacy as "[t]he right of the individual to be protected against intrusion into his personal life or affairs or those of his family, by direct physical means or by publication of information."[44] However, this superficial conformity is misleading because European and common law privacy protection systems dif-

41. *See generally* Directive 95/46/EC, *supra* note 23.

42. *Cf., e.g.*, GUNTHER ARZT, DER STRAFRECHTLICHE SCHUTZ DER INTIMSPHÄRE 101 (J.C.B. Mohr et al. eds., 1970) (providing more detailed distinctions); UDO BRANAHL, MEDIENRECHT: EINE EINFÜRUNG 135 (2009) (distinguishing the social sphere (Sozialsphaere) and secret sphere (Sekretsphaere)).

43. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 194 (1890).

44. COMMITTEE ON PRIVACY AND RELATED MATTERS, REPORT, 1990, H.L. at 7 (U.K.).

fer significantly. The European and U.S. concepts of privacy originated from similar sources in the late nineteenth century but evolved along two very different paths.

Placing the right to privacy in the ambit of ECHR or the EU Charter of Fundamental Rights clearly defined it as a human right, and personal data is considered its primary designation. At the same time, in U.S. doctrine, personal data is perceived primarily as a commercial commodity. This perception is reflected by a strong and rapidly evolving personal data market. There is no uniform federal privacy regulation in the U.S because the government considers it an obstacle to developing free trade and e-commerce.[45] Introducing federal privacy regulations would also be too complex considering the U.S. constitutional regime and the delegation of authority to the states. A unique model regulation developed with the help of the United States Department of Commerce guarantees the protection of few individual rights.[46] The document is aimed at aiding the market self-regulation by establishing a uniform standard for the protection of personal data. It is, therefore, quite different from the European model, which requires governments to take an active role in protecting state residents' privacy.[47]

The inconsistency in privacy perception around the world prompted little controversy until the era of cyberspace. With massive online interactions and personal data retention and exchange, the two different legal concepts of protecting privacy collided, and the need for their harmonization arose. A critical factor for the shape of this globalization was the demanding EU regulation on personal data protection. The stipulations of Article 25 of the EU Directive 95/46/EC on the protection of personal data enforced compliance of all entities collecting, transferring, or processing data protected under the Directive, regardless of their location with the European personal data protection guarantees.[48] Article 25 obligates EU member states to transmit data

---

45. AMERICAN BAR ASSOCIATION PRIVACY AND COMPUTER CRIME COMMITTEE SECTION OF SCIENCE & TECHNOLOGY LAW, INTERNATIONAL GUIDE TO PRIVACY 94–95 (Jody R. Westby ed., 2004).

46. See the Safe Harbor Principles discussed *infra* Part III.E.

47. *See* K.U. v. Fin., 2008 Eur. Ct. H.R. 1, para. 42–43 at 12.

> [A]lthough the object of Article 8 is essentially to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life. . . . These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves. . . . [T]he nature of the State's obligation will depend on the particular aspect of private life that is at issue.

Id. (citations omitted).

48. Directive 95/46/EC, *supra* note 23, at 45–46.

to any state if that state ensures an equal level of personal data security.[49] Therefore, if any non-EU state wishes for its companies or individuals to obtain access to personal data protected under the EU Directive, it would have to guarantee that the data would be protected in compliance with the Directive.

Meeting that challenge proved difficult, especially for the transatlantic flow of personal data. Given the vast divergence between the European and U.S. perceptions of privacy protection, a suitable compromise was difficult to find. A substitute for such a satisfactory compromise was a solution rooted more in business ethics and good practice than statutory law. In order to enable personal data to transfer from Europe to the U.S., the Department of Commerce (DoC) coordinated the formulation of Safe Harbor Privacy Principles. United States entrepreneurs wishing to use personal data protected by the EU law must accept the Principles (an undertaking coordinated by the U.S. DoC). United States entrepreneurs also need to repeatedly certify that they meet the aims declared in the Principles by joining one of the self-regulating programs; for example, TRUSTe or BBBOnline verify compliance with the Safe Harbor Privacy Principles.[50]

III. SAFE HARBOR PRIVACY PRINCIPLES

Following consultations with the EU representatives, the U.S. DoC developed a set of guidelines that satisfied the European data protection requirements.[51] Any U.S. company wishing to use personal data protected under the Directive must adhere to the guiding principles of the Directive, as reflected in the Safe Harbor documents.[52] The declaration of each company to adhere to the program includes an obligation to meet the seven basic aims of the Directive.[53]

Safe Harbor Privacy Principles are not an act of law. Their only legal effect is to encourage voluntary corporate compliance with the Principles verified by authorized organizations. Violations of the Principles are

---

49. *Id.*

50. *See* Henry Farrell, *Negotiating Privacy Across Arenas: The EU-US "Safe Harbor Discussions," in* COMMON GOODS: REINVENTING EUROPEAN AND INTERNATIONAL GOVERNANCE 105–25 (Adrienne Héritier ed., 2002). Additional information about the Safe Harbor Principles is available at www.export.gov/safeharbor.asp.

51. *See* Decision 2000/520, of the European Parliament and of the Council of 26 July 2000 on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, 2000 O.J. (L 215) 7.

52. *Id.* It must be noted that not all categories of data may be transferred under the agreement (health or insurance information are excluded from the regulation). *Id.*

53. *Id.* at Annex 1. These aims include: notice, choice, onward transfer, security, data integrity, access, and enforcement. *Id.*

deemed acts of unfair or deceptive trade practice by the Federal Trade Commission (FTC).[54] In addition, U.S.-based companies operating in Europe may be subject to European states' jurisdiction if they fail to meet their data protection obligations based on national personal data regulations.

The execution and enforcement of Safe Harbor Privacy Principles has been subject to criticism, primarily because of the lack of transparency on the introduction and verification of privacy policies.[55] The 2004 EU review of the implementation of the Principles included repeated concern "about the number of self-certified organizations that have not published a privacy policy or that have published a policy that is not compliant with the Principles."[56] The crucial, practical problem originated from the voluntary character of the guidelines. Since some companies did not introduce any privacy policy, the FTC had no jurisdiction to enforce their compliance with the Principles.[57] The Commission also depicted the lack of a proactive attitude in monitoring organizations' compliance with the Principles.[58] An independent 2008 review showed a growing number of false claims by U.S. organizations on their Safe Harbor compliance and recognized it as a new and significant threat to consumers' privacy.[59] That assessment remains true despite the recent demonstration of FTC authority over Facebook privacy policies that do not conform to the Principles.[60] The 2008 Connolly recommendation for the EU to promptly take "a more 'hands-on' approach" in executing European personal data protection laws abroad was swiftly put into practice in the form of a BCR-based proposal by EU Justice Commissioner Reding in 2011.[61]

IV. BINDING CORPORATE RULES

Responding to growing criticism of the Safe Harbor Privacy Principles execution and the rising threat to European citizens' privacy from online

---

54. *Id*. (in some cases – Department of Transportation).

55. Article 29 Data Protection Working Party, *Working Document on Functioning of the Safe Harbor Agreement*, 11194/02/EN, WP 62 (July 2, 2002), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp62_en.pdf.

56. *Commission Staff Working Document on the Implementation of Commission Decision 520/2000/EC on the Adequate Protection of Personal Data Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce*, at 13, (SEC 2004) 1323 (Oct. 20, 2004).

57. *Id*.

58. *Id*.

59. Chris Connolly, *US Safe Harbor - Fact or Fiction?*, 96 PRIVACY LS. & BUS. INT'L 1, 16 (2008).

60. *Facebook Settles Privacy Case with US Regulators*, BBC NEWS (Nov. 29, 2011), http://www.bbc.co.uk/news/business-15953414.

61. Connolly, *supra* note 59, at 16.

media, EU Justice Commissioner Reding formulated a bold proposal aimed at simultaneously solving both of these problems. In a November 2011 speech, Reding proposed that BCR company codes of practice based on EU data protection standards were the "efficient and effective tools" to properly protect personal information online.[62]

Binding corporate rules, although unpopular, are a well-known practice among European entrepreneurs since their practical application proved costly and burdensome. Those vices preordained the BCR to have a minimal impact on transboundary privacy protection. However, Reding wishes to make them the basis for an amended, legally binding EU proposal governing transnational cooperation on the human right to privacy.[63] Such a proposal would replace the current, non-functioning trans-Atlantic approach.[64]

Although not originating directly from the Directive, the support of WG29 has encouraged the development of BCRs.[65] BCRs are sets of good business practice guidelines adopted by companies voluntarily and applied throughout their branches, regardless of where the branches are located.[66] BCRs and safe harbor agreement declarations differ. Although companies are not legally obligated to adopt BCRs, the rules become legally binding once they are adopted.[67] BCRs become legally binding on companies once approved by one of the twenty-seven national data protection authorities (each for one EU Member State).[68] As Commissioner Reding explained, what follows is an agreement "consciously made" by an EU company to make certain actions vis-à-vis personal data either required or prohibited.[69] The real problem is that approval from one national data protection commissioner is not binding on other national data ombudsmen, leaving a company to struggle through difficult and costly international administrative procedures.[70] Therefore, BCRs are a functional, binding legal tool to prevent privacy invasions and personal data exploitations, not only within EU states' territories, but also worldwide.[71] In her address, Reding proposed a solution,

---

62. Viviane Reding, Vice President of the European Comm'n & EU Justice Comm'r, Address at the IAPP Europe Data Protection Congress in Paris: Binding Corporate Rules: Unleashing the Potential of the Digital Single Market and Cloud Computing (Nov. 29, 2011) (transcript available at http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/817&format=HTML&aged=0&language=EN&guiLanguage=fr).

63. *Id*.

64. *Id*.

65. *Id*.

66. *Id*.

67. *Id*.

68. Reding, *supra* note 62.

69. *Id*.

70. *Id*.

71. *Id*.

by simplifying BCR procedures and encouraging consistency in enforcement and innovation.[72] The simplification of the current BCR scheme would result in its unilateral verification—that is, a set of rules recognized by one national data protection authority that would be automatically recognized in other EU states.[73] To simplify enforcement of the BCRs, Reding proposed strengthening the powers of national data protection authorities to permit prosecution of breaches of data protection laws reflected in the BCRs (with respect to actions within companies as well as third parties).[74] Effective globalization of BCRs would endeavor to show the transnational characteristic of cyberspace in evaluating personal data protection mechanisms.[75] Reding proposes "push[ing] the boundaries of traditional regulatory models" through innovation, not in a technological sense, but rather in a legislative and administrative one.[76] While recognizing that the obstructing EU bureaucracy discourages business from applying the most stringent data protection regulations, the current BCR proposal includes a simplification of administrative procedures for companies that introduce those binding data protection policies.[77] In this sense, innovation means reconsidering the significance of territorial borders in territorial cyberspace. BCRs apply "to all internal and extra-EU transfers of any entity in a group of companies," freeing the enterprise from the obligation to secure approval of the company rules in each country separately.[78] Reding promised the shift would allow companies to operate based on "just one single document that governs the privacy policy of the whole group instead of a variety of different, and not always consistent, contracts."[79]

This innovation is also to be achieved through a revolution in EU data protection. As announced on January 23, 2012, the EU data protection directive will be replaced by a regulation.[80] The significance of this shift in legislative instruments is of tremendous importance. While an EU directive obligates each member state to introduce national legislation aimed at meeting a particular goal as it is defined within the directive, a regulation is applied directly in national legal systems.[81] A data protection regulation would give companies one set of rules to follow regardless of territorial boundaries and would give national data protection bodies the very same system of le-

72. *Id*.
73. *Id*.
74. Reding, *supra* note 62.
75. *Id*.
76. *Id*.
77. *Id*.
78. *Id*.
79. *Id*.
80. *See supra* note 9 and accompanying text.
81. *Id*.

gal rules to apply to every BCR assessment.[82] With the help of WG29 to interpret the prospective regulation and a long-standing privacy protection policy, the prospective shift seems very promising.

The proposal has been met with approval from EU companies and national governments alike. Some states welcomed the changes with coherent, national BCR administrative procedures in place.[83] Anticipating the new procedures, cooperating Danish and Swedish data protection authorities introduced a bilateral formula for approving BCRs in October 2011 and initially applied it to a regional healthcare provider, Novo Nordisk.[84] Similar endeavors may serve as a platform for further harmonization work of WG29.[85]

Reding's idea was designed to be transnational. It is an answer to the challenge of cloud computing across national borders and reflects the specifics of cyberspace. She openly claimed that the BCRs are "open to go beyond the geographical borders of Europe."[86] Should the plans become reality, Europe's leading role in shaping international privacy policy would be enhanced. However, if the bold plan of uniting the global cloud computing market under a joint set of privacy principles of European design fails, what other option could be considered? The most viable alternative is presented below.

V. "WALLED GARDENS" OF PRIVACY

If privacy regulation were left to individual states with no uniform, global standard in place, the internet would slowly devolve from its transnational nature and eventually lose its global character. Building walls in cyberspace is difficult but as the Chinese experience shows, not impossible.[87] Apparently encouraged by China's success in delimiting "the Chinese cyberspace" with the Great Firewall of China, the EU considered the electronic Schengen zone in 2011, the very same year Australia introduced plans to block illegal content away from its "virtual territory."[88] Just recently the

82. Treaty on European Union, July 29, 1992, 1992 O.J. (C 191).

83. *EU: First Nordic Company Secures BCR Approval*, DATA GUIDANCE (Jan 12, 2012), http://dataguidance.com/news_1010.asp?id=1661.

84. *Id*.

85. *Id*.

86. Reding, *supra* note 62.

87. The actual efficiency of the Great Firewall of China is often criticized. *See, e.g.*, Richard Clayton, Steven J. Murdoch & Robert N. M. Watson, Ignoring the Great Firewall of China (June 27, 2006) (unpublished manuscript) (presented at the Sixth Workshop on Privacy Enhancing Technology, Cambridge University), *available at* http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf.

88. *See, e.g.*, Jan Lewiński, *UE chciałaby mieć internet jak w Chinach*, DZIENNIKI INTERNAUTÓW,

U.S. considered closing "U.S. cyberspace" to prevent copyright violations with the Stop Online Piracy Act (SOPA) and the PROTECT IP Act (PIPA). The U.S. is still considering securing "the U.S. cyberspace," as if raising national borders in cyberspace was a natural consequence of state sovereignty.[89]

"Internet filtering" is a term used to describe the national practice of disabling access to certain online content that is deemed harmful by state authorities and is usually recognized as illegal by national laws.[90] Filtering policies are often criticized for a number of reasons. Internet censorship primarily limits the citizens' right to receive information. It also creates a danger of particularization of the global network into smaller, national, well-filtered systems where only some of the global content is available—only as much of it as national laws allow. The vision of an effectively and extensively filtered Internet is sometimes pejoratively referred to as "splinternet," a term depicting the loss of the universality of the network (an Internet "splintered" into separate local webs).[91]

Typically used to control state residents' access to certain data and restrain their right to free speech (which includes the right to receive and impart information), Internet filtering may also be viewed as a limitation on individual rights, particularly the right to privacy. The EU, an organization now proposing a global solution for privacy protection, considered closing its electronic networks to non-EU entrepreneurs with the use of electronic gates in 2011.[92] With the "virtual Schengen border" in place, all electronic content entering the "European cyberspace" is scanned for legality and allowed access only if it meets European legal standards.[93] The idea never made it into a legal bill, primarily due to devastating criticism that it was not only undemocratic but also unrealistic.[94]

This idea should be reconsidered in the context of privacy protection because a splinternet seems to be the only alternative to a globalized privacy policy. The EU is unlikely to stray from its stringent personal data protection regulations. If the BCR proposal does not meet international support,

---

http://di.com.pl/news/38097,0,Opinie_UE_chcialaby_miec_internet_jak_w_Chinach.html (last visited Aug. 6, 2012).

89. *See, e.g.*, Chris C. Demchak & Peter Dombrowski, *Rise of a Cybered Westphalian Age***,** 5 STRATEGIC STUDIES QUARTERLY 32 (Spring 2011).

90. *See, e.g.*, Clayton et al., *supra* note 87, at 22, 33.

91. *The Future of the Internet, a Virtual Counter-Revolution*, THE ECONOMIST (Sept. 2, 2010), http://www.economist .com/node/16941635.

92. Jennifer Baker, *European Legislators Consider Net Filter for Europe*, COMPUTER WORLD (May 3, 2011), www.computerworld.com.au/article/384993/european_legislators_consider_net_filter_europ/.

93. *Id*.

94. *Id*. The inefficiencies and high costs of the Chinese system were the primary arguments against it. *Id*.

the EU will continue its attempts to effectively protect its residents' privacy. Should it find no international accord on the subject of privacy (one that is divergently comprehended in national legal systems), the EU may eventually resort to the introduction of software-based tools to enforce compliance with its rules. Therefore, a privacy based splinternet seems to be a viable option. Moreover, electronic barriers erected for purposes other than privacy protection, such as cybersecurity or copyright protection, could serve as effective safeguards. The EU may resort to building a "walled garden," secured with electronic firewalls—essentially an electronic version of the Schengen agreement. Electronic data would be checked and allowed out of the EU-based electronic infrastructure only if EU laws, including privacy requirements, were followed.[95]

VI. DISCUSSION

BCRs are more effective than privacy protection enforced through electronic walls because they preserve the global character of the network. Perceived through national or regional standards, electronic walls constructed to preserve privacy make the threat of a splinternet real. Regardless of whether it is introduced to protect privacy, prevent copyright infringement, or uphold morality, splinternet signals the end of the global network as we know it. The global information society will cease to exist if the once-global network becomes a set of sparsely connected national webs. Nations may gain the perception of security but lose the interoperability of the global network and access to the global "cloud" of information. If states choose to sacrifice their residents' freedom of information and exercise permanent surveillance of all online activities in order to guarantee security and secure data through national privacy standards, a global cyberspace that posed the initial threat will be gone.

A walled cyberspace does not have to be the answer. International law offers several potential solutions to these global challenges, grounded in its rich jurisprudence on human rights and conflict resolution. There are numerous international projects aimed at reaching a consensus in the application of existing human rights for online interactions—for example, the OECD Guidelines on personal data.[96]

---

95. The practical application of such a scenario is feasible from a legislative point of view; at the same time however, the strong economic ties of European companies with their non-European counterparts make it a final resort.

96. *See supra* Part II.

The more recent developments in privacy protection compromise are geared toward the structure of the cloud-computing based cyberspace.[97] Data protection policies are no longer settled at governmental conferences but, instead, are established by transnational companies. These data protection policies are verified by the users who either willing use them or exit a network they find to be unsafe or exploitive. Global businesses were the first to recognize the characteristics of the information society and amend their policy models accordingly. Because elaborate international hard-law treaties are time-consuming and require extensive compromises, current proposals resort to soft-law measures. These soft-law measures take the form of self-regulation (or co-regulation)[98] based on common ethical standards, described in non-binding declarations or guiding principles. Endeavors such as the Google Global Network Initiative[99] resort to self-regulation, calling upon industry representatives (social platforms operators, ISPs) to adhere to a set of rules and principles aimed at granting international privacy protection to their users.[100] The existing privacy challenge encourages companies to reach for the rich, soft-law background available in public international law. Commissioner Reding's proposal takes this practice a step further, giving a company-proposed set of policy guidelines a legally binding character after its approval by an EU data protection body. Introducing the BCRs might serve as the missing link between soft law regulations and international law making. The role of customary international law is being reinvented.

VII. CONCLUSION

Determining the scope of the human rights catalog for online activities is recognized as the biggest challenge that the information society will have to face in the near future. Success will be realized only if the global community unites to tackle the challenge together. Physical elements of the global network, regardless of their location, may function well only if they are managed coherently. If states fail to see that truth and construct firewalls around the areas that they believe to be their "parts" of the cyberspace,

97. *See, e.g.*, Sophie Curtis, *New Privacy Laws Could Boost EU Cloud Industry*, TECHWORLD, http://news.techworld.com/data-centre/3333104/new-privacy-laws-could-boost-eu-cloud-industry/ (last visited Aug. 6, 2012).

98. The term refers to the multi-stakeholder nature of Internet governance – it is all the stakeholders: the governments, the companies, and the users that must find a satisfactory compromise. *See, e.g.*, *Tunis Agenda for the Information Society*, WORLD SUMMIT ON THE INFO. SOC'Y, ¶ 35, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html (last visited Aug. 6, 2012).

99. *See* GLOBAL NETWORK INITIATIVE (Aug. 2, 2012), http://www.globalnetworkinitiative.org/.

100. *Inaugural Report 2010*, GLOBAL NETWORK INITIATIVE (July 26, 2012), http://www.globalnetworkinitiative.org/files/GNI_Annual_Report_2010.pdf.

thereby creating "walled gardens" to protect their residents' privacy, the global information society will surely face its doom: the end of the global cloud facilitating the free exchange of thought and information. A consensus-based global solution, resembling BCRs in flexibility, may serve as a starting point for finding a global consensus on human rights online protection.